Work From Home: Threats, Vulnerabilities, and Strategies for Protecting Your Network

Featuring Phil Groce 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, 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 and operated by Carnegie Mellon University. My name is Suzanne Miller, and I am a principal researcher here at the SEI. Today, I am joined by Phil Groce, a senior network-defense analyst in our SEI CERT Division.

In this podcast, we are going to examine the threats and vulnerabilities of remote work, which is appropriate since we have all been working at home since March. As a matter of fact, we are recording this podcast from our homes. So welcome, Phil.

Phil Groce: Hi. It is good to be here.

Suzanne: Glad to have you here. We usually start these off by asking you to tell us a little bit about yourself, the work you do here, and in particular, what drew you to this kind of research?

Phil: Right. I work in the CERT Division of the SEI for what is called the Situational Awareness Team, underneath Monitoring and Response. We are concerned with helping people understand what is going on on their networks, the networks that they own, and also how to defend against malicious behavior on those networks. My background, I have spent 15 years at CERT, essentially doing software-development support and analysis for situational awareness. Prior to that I worked in private industry, doing managed security services and intrusion prevention, other things that also contributed to this field for about five or 10 years prior to joining the SEI.

Suzanne: So remote work has been going on for quite a long time, and we have seen quite an evolution in the last six months. What are the things that characterize the environment of a typical work-from-home employee today? Because I know it is different, at least for me, than it was five years ago. What is it like today? And then what are the inherent risks in the way that we are approaching this?

Phil: Well, from a technology standpoint, it is very different than it was five years ago, or even one year ago, honestly. The telecommunications and telepresence technology that exists out there has been supercharged and obviously highly motivated by what has been going on over the last several months. From a network-security standpoint, another aspect that is transformative over the last five years has also been an explosion in the number of devices that exist on home networks. Now you have all these IoT devices, people often will buy and install something that has a network connection that will phone out into the internet and not even know that they did it.

Personal experience: I bought a washing machine a few months ago. I guess it is a year ago now because that is how time passes these days. But we installed it, and it tried to connect to my Wi-Fi. For a lot of people, it would have just automatically connected to the Wi-Fi and it would have used protocols like UPnP [Universal Plug and Play] to make an outbound connection that would allow a central server, with the best of intentions, run by the manufacturer or something like that to contact it. You could have a little app on your phone, and from anywhere in the world, I could see whether I am doing laundry or not. I do not know that that is necessarily the most valuable use of the Internet, but for a lot of people it probably has some value. But the point is that it would automatically do that without anyone thinking about it. That gets to something that has not changed in a long time, and really has been true ever since people start installing things in their home, and that is that these networks are not professionally managed. There is an explosion of devices, which obviously a lot of people are not even aware are there, and as those devices get installed, they age. So another thing that has happened over the last five years is that all the things you installed five years ago got five years older. For a lot of people, those things are working just fine for them, and I will use quotes to indicate that they are working "just fine" because they are doing their jobs. But a lot of them are not automatically being patched. The advent of automatic updates was in progress five years ago, but it was not nearly as ubiquitous as it is now. So a lot of these systems have not been updated in years because they were, scare quotes, "working fine."

Furthermore, some of them have even become completely end of life. What that means to a device is if you are not receiving any more updates, and someone discovers a security vulnerability in the software you are running, it is never going to get fixed. So that leads to the notion…there is a class of vulnerabilities now that are…we have the notion of zero-day vulnerabilities, which people have probably heard in the context of the news like Stuxnet and things like that, and those are vulnerabilities that exist in currently patched software. They are

really scary, because anyone who has access to one of these can use this to exploit software, even if it is completely patched up. Those are really scary vulnerabilities. There is now a category of vulnerabilities called infinity-day vulnerabilities. These are vulnerabilities that have been discovered in end-of-life products that the manufacturer is never going to fix. So they exist forever. As time goes on—and what we in the industry sometimes call bit rot continues—then you can expect the number of devices that are exploitable by these infinity-day vulnerabilities to grow and grow. In a professionally managed network…I was thinking about my job the other day, and it occurred to me that the majority of everything that I do, or the majority of all the practices that I advocate, is essentially just cleaning up, taking out the trash. Just like you would clean up your kitchen every single day, or you do your laundry every week, you have these regular tasks that are involved in keeping your network hygiene up. In a professionally managed network, a big part of that is auditing all of the assets in your network, and making sure that everything that you are maintaining officially has up-to-date software on it, so that it is not vulnerable to vulnerabilities. Also, that stuff that is no longer maintained is removed and upgraded, replaced, or just taken out because it is a vulnerability and a risk. That does not happen in a home network.

So a lot of what has been going on—to bring it all the way back—in the last five years is a huge transformation and a huge explosion in the number of devices on, and the complexity of, home networks. But at the same time, the same thing has been happening, people are not professional network administrators at home, nor should they have to be. They are not able to perform all of these tasks because they have jobs, I have a job, you have a job. It is not network administration, and when it is, we deeply resent it. And as a result, over the course of time, these vulnerabilities are accumulating and building up. At a statistical level, they are inevitably building up into a groundswell in home networks across the world, really.

Suzanne: What this makes me think of is my network quite frankly and reflecting on what you are talking about in terms of bit rot. It is like, *Gee, I wonder how long ago was it that I called my provider,* I will not name them, and said*, Hey, is it time for us to do an upgrade?* Of course, from their viewpoint, the longer a device that is managing the network is out there, the more profit they get whenever they have to replace it, etc. There is really not a lot of…I have received nothing, I will just say it that way. I have received nothing from my provider that says, *Hey, it is COVID. We know everybody is working from home, and you should take a look at these things on your router and make sure that everything is up to date. If it is older than x date, then we should replace it.* We are not getting those kinds of notifications. Maybe some providers are, but I am not getting it from my provider, and it is a first-tier provider, so I am kind of expecting that is the norm.

Phil: Yes, it is a serious challenge. At this point I think a lot about how this technology environment should translate into policy. I think at this point, I am pretty much convinced myself that our policy stance toward this should be that we should not expect home-network owners to responsibly manage their networks. It is what we really want to do. If you are a home-network administrator, please go do what I was talking about, upgrade all of the devices that are out of date, get rid of the ones that are end of life. For the love of Pete, please go to your Internet router and make sure that it is fully supported and is fully patched. That is probably the most important part of your home network at this point. And buy a new one if it is outdated. If you are still running a Linksys WRT router from the early 2000s, update that.

But, at the same time, our default assumption should not be that home-network owners are going to properly administer their network. We have to defend our enterprise networks and other networks with the assumption that those are going to be vulnerable. I know that the other side is doing that, because that is the sort of thing that you are going to see if you start looking at threat-intelligence companies' websites and start reading about the way that ransomware attackers and people who use botnets, things like TrickBot, that are sort of exploit kits. All these unpatched devices are chum in the water for a category of sharks that live out there to attack. I generally divide the world at that level between two categories of attackers. To draw an analogy to just petty crime, there are the opportunistic attackers, so the guy who is walking through a parking lot and just jiggling the handle on every car door just to see if there is one that is unlocked. And if there is, they will get in there, and they will see what they can get. Maybe it is nothing. Maybe somebody left their phone in there. But the primary modus there is, *We'll take whatever we can get from whatever is available.*

The contrast there would be a targeted attacker. So, I think there is a ready analogy there. We readily understand what that means in the information-security world. In the criminal world, it would be something like an estranged relative who is a stalker, for instance, or someone else like that, who is definitely trying to get *you*. Obviously this bit-rot condition that we have in home networks has attracted a lot of opportunistic attackers. So, the majority of infections—you know, the metaphor we always use—the majority of infected machines or exploited machines, compromised machines in home networks have probably been compromised by opportunistic attackers, and they really have pretty low standards when it comes to what they want to do with this. They want to maybe make your machine part of a botnet, they might want to send some phishing or spam from it, not specifically directed at who you are, the fact that you work for some important company, and you work from home every day.

But one of the things they are going to do is go on websites that they have that they can go to that represent marketplaces, and they are going to try and resell some of these compromised devices, either as part of a botnet, or perhaps just saying, *I have popped all these different things. I do not*

even know what they are. I have done some really basic due diligence. I will sell the credentials to access. They all have a remote-administration tool of some sort on there, and I will sell the credentials to access these 10,000 machines for however much money, right?

The targeted attackers know that. A lot of those represent organized crime. Ransomware increasingly is being performed as an organized criminal activity. It kind of has to be honestly, especially when it comes to getting people to utilize cryptocurrency. They have actually had to stand up support desks; that is how organized this crime gets. Of course, if you are high enough on the food chain, if you are, say, working for the government, or if you are working for a very large corporation, if you make a high-value target, then you are going to attract the attention of the so-called advanced persistent threats, or state actors, or other entities that are interested in very specific and sophisticated kinds of attacks. They know these opportunistic attackers are out there, and they know these marketplaces are out there.

By opening yourself up to these opportunistic attacks, you are opening up a vector of attack for a much more serious kind of attacker. Now, whether that is important to you specifically, personally, depends a lot on who you are and who you work for. But if you are a large enterprise, and you have thousands of remote workers out there, the probability that one of them is going to follow this admittedly fairly improbable attack chain, starts to approach a significant fraction, and it actually starts to become a risk that you are going to have to model and mitigate.

Suzanne: There is that side of the vulnerabilities that are inherent in the access, the home network itself. There is also the side of what are the solutions that we are starting to use that we may never have used before for doing remote work? We are using things like virtual whiteboards that allow multiple people to access a website, essentially at once, and do work. We are trying to educate our children and use rich graphics and learning-management systems, and things that we, from the home viewpoint, may never have included in the things we thought about how secure are these kinds of tools. Zoom! You know, we are using Zoom right now. And then there [are] lots of others, and new players in the collaboration marketplace. Some of the other tools are adding collaboration, *Oh, you can use our tool, but then you can also, instead of just doing text chat, you can do video chat*. So what is the effect on security of all of this explosion of remote work tools, and how do people evaluate whether something that their teacher wants them to use, or their work wants them to use it, or their customer wants them to use—how do you evaluate the security of those new things that you have been exposed to?

Phil: That is a really good question, and usually, when we say things like, *That is a really good question*, we mean that the answer is really not going to be very pleasing to anyone. Oh yes, all right, raise your hand! I mean, it is the truth. But no, that is a good question. I mean raise your hand if you knew what Zoom was this time last year. I am going to put my hand down because I didn't know. There has been a profusion of them.

Suzanne: Myself.

Phil: Yes, exactly. There has been this profusion of new tools that have been thrown at us. The toughest part of this is us knowing when these things present themselves as solutions to a real problem that we have, a series of real problems that we have, being able to evaluate what is the effect that this is going to have? From a personal standpoint, I would say that the number one concern I have as an individual is the privacy of my data. I am concerned when I hear that, for instance, a communications company has not respected my data by encrypting it enough, or by sending it into jurisdictions that might have rules about data privacy that are not as up to my personal standards for what I want in terms of my privacy of data.

So, I think that that is a significant concern that we should have as individuals, [which] is learning more about the tools we use and how they intercept data. But I think that as an individual, I think a lot more about things like smart speakers and smart TVs when I think about things like that. To a lesser extent, I think about things like what we are using now, like telecommunications technologies, that we are maybe having confidential communications on. Maybe these days, we are having medical conversations via telemedicine over Internet lines and the standards that people use for storing that data, for transmitting that data, and for disclosing that data, who they disclose it to and why.

Fortunately, I think that in America, we have thought about health-information privacy a fair amount. So I think that there are certain areas of our lives, where if an organization, a reputable organization like a large hospital or medical-services provider asks you to use a certain piece of technology, most likely it has gone through a very rigorous process where it has been evaluated and determined to preserve privacy in a number of fairly specific ways. You can always, as an individual, spend as much time as you have to go dig down and see what the actual details of that are. If you are like me, Susie, you frequently just have to trust, and I think that we are in a better position to be able to trust stuff with, like, our medical and our financial information, than a lot of people are in a lot of parts of the world, maybe not as good as some, but better than others, and enough that I personally, as just a trust decision, feel comfortable if my medical provider is asking me to use telemedicine or use a secure portal of some kind to exchange information with them. I can feel relatively comfortable about that. When it comes to the point of, like you said, school districts evaluating technologies in order to provide them to their children, they similarly have a duty of care. I will say all, as close to all as makes no difference, take that very seriously. So I think in some ways you can establish the same level of trust. I do not think you can make quite as strong a trust guarantee only because they have the best intentions, but they do not always have as much oversight in terms of what the process is like for their evaluation. They do not always have as much technical expertise available to them.

Suzanne: I actually know someone who, as a volunteer, went out to a family's school district that was not where they live to do an evaluation of their learning technology for them because they did not have the money. When he was asking about his nephew's schooling, and he is hearing all these things that are like *OMG! I will come on out. I will come out for a week and help you guys*. Which is wonderful, but it is also telling that there is that variability in some areas that we want to be able to trust, but there may not be the skill and the resource and the capacity available to actually give you that sense of trust.

Phil: The SEI has famously created the Capability Maturity Model, and the lowest level on that model is characterized by personal heroics. It sounds like your friend was engaging in personal heroics.

Suzanne: He definitely was, and thank you, but it was a little bit unexpected for me. I do not have any children in school, and so I am not living through all of this right now. So I had not realized just how much it is affecting the whole technology base of the education system that has been geared completely away from that until very recently. Work from home, telecommuting, 10–15 years it has been a thing in the workplace, but it has been the exception rather than the rule. Now, I think we are going to see a lot of changes in work in general once restrictions from COVID are actually lifted. You are going to see a lot more of that on a regular basis.

The idea is that we need to take responsibility for our…an enterprise needs to help the people that are working from home take responsibility, and by giving them solutions that are trustworthy, and people at home are going to need to take more responsibility for their own situation to make sure that they do not add risk into the milieu for themselves and for the enterprises they work for. I think that whole ecosystem is really changing, and it will be interesting to see what happens because that changes the social aspects of work as well as the technical aspects of work. That is another conversation.

Phil: It is a fascinating conversation. I think you are right that the technologies that we are being exposed to now are going to be with us for a very long time, and they are going to be with us at all the levels that we are experiencing them, not just work, which obviously, I think a lot of people have found that the results of this, people are making substantial investments in remote work. While there are significant costs involved, they are being forced to undertake those costs, and they are in a position to realize the benefits and the cost recovery. There are a lot of companies, like Twitter and Slack are obvious public examples, that have already said, *We are not going back. We are going to sell our real estate*.

Suzanne: Yes. I found in my own personal situation, my father is 91 years old. Before COVID, I had been able to see him, go out and visit him physically, about every two months. I have not seen him since February in person, but he was one of the early adopters of Zoom. It is like, *All*

right, we are doing Zoom calls. I think he was probably one of the ones that got his church to do Zoom services and things like that.

So people are adjusting to get the social connection that they need, in different ways than we have before. The cascading effects on industries, like the airline industry and things, we do not know what those are going to be yet. I want to switch us back to some takeaways, and one of the things the SEI does for the world, and CERT in particular started, is providing information publicly about what can you do about threats that we identify, vulnerabilities, make us aware of them, like this podcast. Then also, *Here are some things you can do about them*. What are some of the resources that are available to people, if they want to come to the SEI CERT website, the SEI YouTube channel? Are there things in particular, you would say, *You probably want to look at this. And here is what we have for you.*

Phil: There are lots of resources on the Internet that I encourage people as individuals to go out to, and I think a simple Google search about how to secure your home network is actually pretty revealing. It is all pretty basic stuff. The problem there is not that the knowledge is not out there. The problem is that people do not have the time and people aren't necessarily pushed. There is not a little sticker on your router that says remember to check it every six months. There is not a best-by or a sell-by date on our routers.

Suzanne: Like our milk.

Phil: Yes, well, milk has a very nice natural way of telling you it is time for you to buy new milk.

Suzanne: That is also true.

Phil: That doesn't exist for a lot of this technology, but once you just start to scratch the surface there, it is fairly simple. Look at your devices. Try and find serial numbers, go Google those serial numbers.

Suzanne: That is a sign if you cannot even find a serial number.

Phil: Yes, it is probably a little like the smell of your milk. So if you want to really try and harden your network against attack, I would start with your router. I would go and I would look at the connection to the Internet. There [are] probably two ways that you are connected to the Internet. One popular way is to just let the cable provider or the Internet service provider provide you with, they call it premise equipment. Part of the job of that premise equipment is going to involve routing you out to the rest of the Internet. All you are supposed to be expected to have to do is plug probably a switch or something, because you probably have more than one thing you want to plug into the Internet. Or maybe they have multiple ports on their own device and you

plug all those in and you are done. You are up and running. In that case, that particular device is the responsibility of your Internet service provider. Now they may have rules and regulations or things that state that it is your responsibility to do this or that, and you should probably just go ahead and have a conversation with them.

Suzanne: Change your password from 1-2-3-4 to something else.

Paul: Some of them do not let you do that.

Suzanne: I have to remember to remind people to do that because I still run into people that when we are talking about this stuff, I say, *Well, when did, when was the last time you changed your router password?,* and they go, *What?*

Phil: Yes, absolutely, and why should they just automatically think that this thing has a password? Especially if it is just a physical black box that you plug things in? Why should my washing machine try to get on my Wi-Fi, right? Have a conversation with your Internet service provider, especially if it has been a while since you have had your Internet service installed, and ask them. Look at the model of the thing you are plugging into, find a serial number or something and say, *Is this the most current thing you are installing? Are you guys maintaining this? Should I get a new one? What are my responsibilities with this? What are you expecting me to do to keep this thing secure and up to date?* Depending on those answers, or if you are a nerd like me or you, then you might want to go and get your own router, maybe you got your own router years and years ago. Maybe a nerd like me is your son or your brother or something, and they installed one for you. If you are in that situation, then you do not have an internet service, the internet service provider's not going to give you the time of day on that guy. Just go to the internet, that serial number is going to be very valuable in finding the documentation about the device, probably people who have owned that device, and you can find out, how old is it? How well maintained is it? Are there more current updates for the software or firmware that runs on that device? How do you install that? Then you can make a decision for yourself of, *Should I commit to keeping this?* If so, then you need to commit to updating it. Or, *Should I just go get a new one?* You can make that consumer decision a bit more informed as a result of that. Unfortunately, once you get further into your network, and you get more and more devices in the network, then things become a bit more daunting. The more advice I give on that, the more it starts to look like you become a professional network administrator. You have to draw a line for yourself.

Suzanne: It is a balance.

Phil: Yes, you have to say to what degree am I willing? Honestly, a lot of people find it to be a fun hobby to administer their networks. Well, OK, I do not know if a lot of people do. I do.

Suzanne: There is a segment of the population.

Phil: Yes, there is a weird segment of the population like me that likes to do that. If you like to do that, and if you find it is…What working on cars was to my dad, working on networks is to me. If you are like that, then I do not need to tell you, you will get fascinated by it, and you will go in, and you will find all the things you need to do. If you are like most people, at a certain point, you are going to look at this, and you are going to say, *OK, good enough*. I would say that at a very bare minimum, everyone needs to feel good that their router is up to date, and the responsibilities that they have with respect to it are being met. Then go all the way to the other side, and look at the actual devices you use almost every day.

That brings us actually into the enterprise, because a lot of us are remote workers. We are connecting using various connection technologies and various devices. There is kind of two breakdowns there. One is what hardware is provided, and one is the software that you are using to connect. So, a lot of enterprises historically have provided their employees with enterprise equipment that has been shipped to the user from the enterprise, or they maybe directly got it from an IT person, maybe when they joined the company, or last time they did a tech refresh. That is a professionally managed device. One of the challenges that enterprises have had over the last several months has been to maintain that level of professional management. By and large, I think they are pretty familiar with what the best practices are there, but there have been a lot of time pressures and a lot of challenges where enterprises have had to maybe take some shortcuts, and I have some advice for enterprises too. But as a user, if you have an enterprise-maintained machine, I think the most important thing for you is to follow your enterprise's instructions with respect to that. That may mean that you have it connected to the internet so that it can receive updates. It may mean that you have to log in using a remote-access solution for a certain period of time, so that you can receive updates, but just listen to your IT people and follow the directions with respect to that.

Some people are using "bring your own device," BYOD, or end-user devices, and this has become an increasingly popular solution in the last several months because a lot of people had to turn on a dime, and they did not have any budget for furnishing all of their workers with remote equipment. So, they have sought technology solutions that would permit them to utilize people's pre-existing, end-user equipment, which can be a real hodgepodge. We were just talking about the fact that people are not professional network administrators; they are also not professional system administrators. The variety of operating systems is wide, the variety of currency of operating systems is wide.

There was one survey that I was aware of where fully 10 or 15 percent of the inventory of enterprises that were connecting to their remote-access solution were running Windows 7 and Windows Vista, both of which are end-of-life systems. They are not being updated. They have

these infinity-day vulnerabilities on them. And they had to do that because they had to transition to remote work on a dime. Enterprise folks, do not beat yourselves up on this, but at the same time, you are not done because you have released a remote-access solution. The remote-access solution has some security built in. Most likely, you have evaluated that when you were acquiring the solution, and it probably has some things like multifactor authentication, which are very good to have.

There is a type of remote-access solution where the user connects to a device that is actually resident in the enterprise, that just starts up a virtual machine. They work on that virtual machine all day, and when they log out, the virtual machine is deleted, it is destroyed. Those are virtual-device infrastructure solutions. There are different ways to configure it, but that is one of the more secure ways. It is certainly a positive thing to do for security, because it makes it harder for attackers to gain persistence in your network. I think you can regard that as the beginning, but not the end of the matter.

Because at the end of the day, if an end user is using a vulnerable endpoint to access your solution, even indirectly…Another common thing that enterprises do is they release—some might call it soft laptops—they will use virtual machines and distribute virtual machines to their employees. The virtual machines may be a full machine that is using a VPN to connect to the enterprise, or it may itself just contain a remote-access solution that is a bit indirect. That provides another level of isolation, but it does not solve the problem because that machine is still hosted on another machine. That machine is living in a home network, which as we have discussed, is an extremely vulnerable place to be. If it is not properly patched, then an attacker gains persistence and they have a persistent vantage point from which to mount as many attacks as they want until they succeed, and they only have to succeed once. So, you have to worry as the enterprise about the safety and security of the machines that are used to connect into your enterprise. What are the tools for doing that? Well, there are a few.

Another one of those things that I think has exploded in the last year, although it may not be as visible to end users, is device management. Device management really sort of came into its own as people wanted to start using their fancy new smartphones to read enterprise email and things like that. IT departments had to find a way to say yes to that and still maintain a security posture that they felt comfortable with.

So device management started out mobile-device management, a lot of them. What would happen here is that you would install this app on your phone, for instance, or your iPad. It would enroll you, so it would connect to a server in your enterprise that is dedicated to this from the internet. You would provide some credentials to establish your bona fides with the server. Then once it did, it would actually start to control certain aspects of the configuration of your phone or your iPad or other device. This allows an enterprise to—I always call it projecting policy—it

allows them to project a policy outward and establish a safer space or at least be able to negotiate a risk profile that they can be comfortable with around that point of connection, to assure that like if data is passed over, it stays in a certain place, and you have to be a certain person in order to see it. You can't copy it off the device into an untrusted area or something like that.

These device-management solutions were already there, and they were growing and evolving because the natural tendency is to want to use one tool for as many things as possible. They were already evolving into the larger device space. So, laptops, workstations, that has become supercharged over the last year as you can imagine, because laptops are every bit as much remote equipment now as phones were. They have branched out, and there are products out there that exist to apply with a number of different applications. The same exact system can be applied. You can even do enrollment from outside the network. So someone with a Windows laptop or a Windows machine at home that they are just using can go and enroll, and then something can be sent down to their machine that will control certain aspects of the configuration, and might actually validate their configuration. *Oh, you are running Windows 7? No!*

Suzanne: *No, we are not playing with you*!

Phil: *Sorry, you are going to need to upgrade this machine.* That is an important part of, as an enterprise, policy enforcement and policy projection. The other big tool that I would argue is pretty critical, is what they call self-service tools. These grew up around IT departments wanting to run their business more efficiently.

The approach anyway was to turn a lot of their services around and automate them so that end users who have problems can get solutions without having to really make substantial contact with a human being unless they had to. But a big part of that is making new enterprise software available to end users. Well, it turns out that is a really important thing to do to a remote worker at this point. There are lots of really important enterprise security tools that you can deploy using this channel. For instance, endpoint monitoring or a secure VPN that may have your credentials on it and things like that.

Regardless of your remote-access solution, it is not the whole answer. And a lot of people have deployed remote-access solutions and gotten people up and running and working remotely, and their business is still a going concern. And availability is a security property. You have done a good job, but you are not done yet. As things are calming down, look around you. Look at the statistics of the systems. A lot of the remote-access solutions collect statistics on who is connecting to them, and what systems they are running on and things like that. Look at those. Identify systems that are end-user systems that may not have a configuration that matches your risk tolerance. Then look at these solutions for projecting your own policy out onto those

endpoints, and think about how your own policy needs to change to incorporate those tools and solutions. Technology is never a substitute for policy or process.

All of these things that I am talking about, if we talk about new technologies, what we are really talking about, before we even get to that, is thinking through the policy that you want to institute and the kinds of processes that you want to support. Then, when you are done with that or in tandem with that, you consider these technologies, these remote and self-service technologies and device-management technologies, as tools to help you implement those policies. This is a great time to be thinking about that. Now that we are past the main tidal wave of transition, now it is time for consolidation and standardization and professionalization of the whole thing. So get to work guys.

Suzanne: And that is why we are talking to you.

Phil: Thanks.

Suzanne: I really do appreciate this insight. I know I am not a professional network administrator. But I [have] a couple of things on my list of things to do to make sure that I am being a responsible enterprise user, and I think people that are in the professional realm may be now ready to take a breath and listen to some of these ideas where, in the first two months, all it was about was making sure the network did not crash. As you said, we are kind of beyond that tidal wave, so now it is time to think forward.

I want to thank you very much. I look forward to talking to you about other areas of your research because I am sure you do other really interesting things. Today, it was all about the remote work. It is all about us remote workers today. I want to thank you. I want to remind our audience that we will include links to resources that we mentioned or that we think are useful in relating to this question. If you have any questions, as a viewer, please do not hesitate to reach out to us at info@sei.cmu.edu. I want to thank all of you for joining us today.

Phil: Thanks. It has been a pleasure.

Thanks for joining us. This episode is available where you download podcasts, including SoundCloud, Stitcher, TuneIn Radio, Google Podcasts, and Apple Podcasts. It is also available on the SEI website at sei.cmu.edu/podcasts and the SEI's YouTube channel. This copyrighted work is made available through the Software Engineering Institute, a federally funded research and development center sponsored by the U.S. Department of Defense. For more information about the SEI and this work, please visit www.sei.cmu.edu. As always, if you have any questions, please do not hesitate to email us at info@sei.cmu.edu. Thank you.