Defending Your Organization Against Business Email Compromise

featuring Anne Connell as Interviewed by Suzanne Miller

Welcome to the SEI podcast series, a production of Carnegie Mellon University's Software Engineering Institute. The SEI is a federally funded research and development center, sponsored by the Department of Defense and operated by Carnegie Mellon University. Today's podcast is going to be available at the SEI website at sei.cmu.edu/podcasts.

Suzanne Miller: Hello. My name is Suzanne Miller. I am a principal researcher here at the SEI on the Agile-in-Government team. I am here today to interview Anne Connell, who is a cybersecurity engineer over in our CERT Division.

Today, we're going to talk about business email compromise in all its many forms. I'm excited about that because I get crazy business emails, and I know we do a lot at the SEI to try to defend that. But we want to find out more. Before we get into that topic, just tell us a little bit about how did you get into this kind of work? What is it that you do here, and how did you get to the SEI?

Anne Connell: I started off working in the CMU School of Design. Really, I worked there for about 10 years as the network manager. A lot of the faculty, especially because they tended to be older, and phishing isn't something that just came about. It's been around for quite a while. That was the first taste of seeing people get taken, responding...Malware on their computers and/or for them, it was everything related back to the virus that you know, CERT famously discovered...

Suzanne: The Morris Worm.

Anne: The Morris Worm. I'm not saying it was the Morris worm, but it was, indeed, a lot of them getting phished. It's interesting. I'll never forget the one faculty member. I won't use his name, but he said, *I got an email, and they told me that I had money in this Swedish bank account*. I had to ask, *Do you have a Swedish bank account? Did you ever open one? No, no.* I said, *Well, then it's probably a scam*. And to them, it really was, *Why, why would people even do this*?

I was pursuing my degree while working there, my master's degree in human-computer interaction. While there, I just wanted to actually use it more so than just managing computers and setting up machines.

I took a job here at the SEI working for what was the team before STEPfwd on creating training for the SEI and for all its customers.

Shortly after that, there was something. It was the group headed by Rich Nolan. It was the Digital Intelligence and Investigations Directorate. Working with them, they had a lot of law enforcement, Federal law enforcement liaisons. Initially, I was working on the projects, kind of creating web apps for them to access tools and training. Then it became much more interesting to work with them on requirements gathering for these tools. In doing the requirements gathering, you really got to see the problems that they were dealing with. That's sort of my path into this work now.

Suzanne: OK. So, let's talk about business email compromise. We have had everything from the historical Nigerian prince that I think everybody in the world has seen, at this point. Up to more recently, something like Operation Wire Wire, which was a scam that involved like $14 million in fraud, so really big numbers. This is something that has been around a while, hasn't gone away, so we need to deal with it. Your work is doing that. Tell us a little bit about what are the types of business email compromise that we can be looking for and especially, what are the ones that are more insidious?

Anne: I am really glad you said the Nigerian prince because we have come a long way from the Nigerian prince to, in fact, the Operation Wire Wire and that Nigerian criminal ring. Again, Nigerian.

Suzanne: Hi, Nigeria.

Anne: We've come a long way, but there is a lot of things that are the same. The attack vectors that I want to talk about are there is the CEO scam. They are all scams, by the way. Business email compromise is really just a fancy way of saying sophisticated scam. So, it's CEO, CIO, good old social engineering, and/or brute force, lawyer impersonation. We also have the romance kind of scam developing a relationship over time.

The CEO scam, that's when a relationship is built a little over time where they get in on the network. In this case, the company, they infiltrated the network buying credentials on the dark web. Then basically just kept trying, because they could have 100 attacks that they are launching. Only one needs to succeed. They jump around the network. They obtain domain admin access. Then they can find out how the email servers work, whether it's digital signatures or the signature just on an email. Indeed, they can see who works for who and find the best way to target someone who might work for that CEO and be able to impersonate them. The instance here—the one that I talked about first before Operation Wire Wire—was the Texas Energy Company scam. That was a young man who went by *Colvis*.

That Texas energy company, he selected it simply because there was a direct flight from Lagos, Nigeria, to Houston, Texas. We'll come back to that eventually, because I think it's really interesting that his criteria for conducting this was based on a direct flight. It was easier to go to Houston and more cost effective for him than to fly all the way to San Francisco.

Essentially, he was already working with pre-established money mule groups, so that had a lot to do with the areas in which he was interested. He selected this energy company and pretended to be the CEO, sending an email about three o'clock on a Friday pretending to be the CEO, sending it to the person who would process the wire transfers. Sending an email directing them to do it today before close, and that he would be unavailable this weekend. In fact, they social engineered his Facebook page to find out that he was the coach of his daughter's soccer team, even that she was going to have a game on Sunday, *So don't contact me,* really extensive work into finding out the best way to make this convincing.

Even in the signature, he included the same terminology that typically their vendors would use in their invoices. It really was a convincing story and communication that turned out to be then a wire transfer of $3.2 million dollars outside of the company to a fraudulent account. That particular case, we are talking 2013-2014. *Colvis* wasn't his first name. It was his middle name. They were able to find him because it happened to be his Instagram handle. The same way in which he was using social engineering to find more information about his target to make his scam more convincing, they used social engineering to find him.

This is just a really interesting fact. He had already applied to go to the University of Maryland, Baltimore County to study architecture. He actually had come in, I am guessing for the interview. They tried to intercept him that time, but the supervisor, special agent in charge of the investigation, just happened to be out on maternity leave. So, she missed him that first time, but he had applied for a visa. On his second time, and that's when they were able to intercept him. He stood quiet for quite a while, but they eventually got information from him about the criminal ring he was working with. That is a very thorough example of the CEO impersonation.

There is also lawyer impersonation. That is to intercept, say, huge payoffs for a home, especially when you're buying a home. You are sending that initial down payment, whether it's 20 percent that's required. They will pretend to be the lawyer that is taking care of that transaction. There is also just regular social engineering, finding out somebody who might be an attractive target. You can even really assess their level of sophistication, their tech savvy, by how they interact with their social media. There is that, establishing communication with them, pretending to be one of the vendors, and reaching out to them.

That is how a gentleman, in the scam that was Qantas, he was able to get $100 million out of Google, Facebook by pretending to be that vendor and sending fake invoices to these companies

including a wire transfer [asking] for specific information, so that it would go to these fraudulent accounts. So, really, tech-savvy companies. We're not just talking about energy companies. We're talking about Google, Facebook. They're falling for it. It all depends on who you get to, what level of employee, which is why organizational training and awareness is so important. There are also romance scams. There are also lottery scams. There is theft of your W-2 information and your tax returns. There is a lot that is done.

Suzanne: I actually know somebody who… Their tax return was intercepted. They went through all kinds of stuff with the IRS to get that resolved and...

Anne: The work that happens for these victims. I mean, it's regular people.

Suzanne: It costs a lot of work and, and trial for the victims. I also had another colleague who was a victim of—I think this would be the social engineering—*I am in London, and I lost my passport, and I need $1,200 to get home*. They sent this out. They got his email list and sent it out to a dozen people, and three of them sent money. Three of his friends sent money to this fraudulent account. The plausibility, I think, is really the work goes in on their part into making it plausible, because he is somebody who does travel internationally, and he is a little bit absentminded professor.

Anne: They are counting on that.

Suzanne: Him losing his passport wasn't something that people would say, *Oh, that would never happen*. I think that is the key to a lot of these is building the plausibility. How do I as an employee in a company that interacts with lots of different people—SEI interacts with a lot of different people—I don't control money or anything, but how do I protect myself from being compromised by these people that are really good at building these plausible scenarios?

Anne: That is a really great question because even we here at the SEI—I am sure we have tons of network appliances in place to try to prevent these attacks from happening—but all of those appliances, right, are very sophisticated, looking for malware, looking for viruses. You might have three firewalls in place, and a lot of this stuff just pings off of that. It doesn't even get to us.

The difference here is the attack method isn't very sophisticated. It's that our data is out there and the fact that users are under attack. It's not difficult for somebody to actually have this happen, even somebody here at the SEI again, again the Google and Facebook. You would think that there would be more organizational training and awareness since this is number five on Gartner's list of the types of attacks that are the most common attacks and the most devastating. Basically, the IC3, which is the Internet Criminal Complaint Center, they record these incidents. They are largely under-reported because organizations and companies...

Suzanne: They don't want everybody knowing that they got taken.

Anne: They don't want to talk about the breach that might have happened. They don't want to talk about how much they got taken. They don't want the hit to their brand, because recovering from these things is pretty…It's not just the $3.2 million that goes out the door. It's also then the loss of recovery, the, *What data do we need to purge? How did they get in?* Then there is the remediation of both the, your network rules and how you train employees.

All of that is pretty disturbing when you think they are still concerned about the loss of productivity at the same time. *Maybe we shouldn't train everybody because we don't want people not doing their work, too*. They wouldn't want to lose four hours for every individual. There is a lot of tradeoffs that take place.

My point is that it is a lot more than just the take. These scams are so lucrative because you can tie that money into pretty much a little bit of work and a lot of return. It's incredible what they actually are able to succeed with. They don't have to go and purchase Block on the dark web or do social media mining. They can do it above board. In any case, these kinds are ridiculously, as I said, lucrative. They is also the fact that they are increasing. They increased 136 percent from December 2016 to May 2018. That 136 percent totaled about $12.2 billion in take.

Suzanne: That's with a B.

Anne: That's with a B.

Suzanne: This is something we all have to take seriously. Now, I know that one of the things you have done to help with this is to build a data privacy guide. How is that something that organizations can use to help them avoid being one of the ones taken in this, in this kind of an environment?

Anne: The last revision of the, the NIST 800-53, rev 5...

Suzanne: That is the Risk Management Framework.

Anne: That one, essentially, that allowed for some security controls to be put into or recommendations to be put into networks to start to consider data privacy. But the idea of those security controls also…It's not only looking at information systems but dropping the word *information* and just including *systems*. That is a lot better approach because we are now thinking about not just here in the network, your work network, but all of the devices which you connect to that network, and policies as they relate to your phone, your tablets, your laptops.

The idea of agreeing to maybe a little bit more sophisticated user-monitoring policy. The access policies. Just largely, lots of things learned from breaches and taking these security controls and

sort of upping the ante to understand where they should be implemented and with what corresponding policy. That is one of the ways in which it is being addressed. It is going to take a long time for that, those policies and those recommendations to be implemented.

Largely though, most organizations have some impact on this. They have done some work, so hopefully this is just another iteration. The problem with these particular types of compromises, and the way in which this isn't going to decrease, is because larger companies, organizations are putting these controls in place and building on what they already had, the incremental change, they are now hitting small-to-medium businesses.

Suzanne: They don't have the money. They don't necessarily even have a network analyst. So, they don't necessarily have the structures in place to protect themselves.

Anne: Right, and they're operating lean and mean. They don't want to spend a lot of money on this. What they are doing is, maybe they are using Office 365. Maybe their administrative assistant is the same person who processes invoices. They are hitting them because money is money.

Suzanne: They don't care where it comes from.

Anne: In fact, there is still use for the dark web in that there is even these convenient credential - stuffing applications. They can even filter, compare that list to say, the Forbes Top 100 CEOs. They can tailor their searches, so that they can find who are the best targets. Maybe they will eliminate the top 50 because they know those companies already had a breach. *Let's move on down. Maybe our take won't be as much, but maybe we can do more and get the same amount again.*

Suzanne: In aggregate, yes.

Anne: In aggregate. Right. Again, these are lucrative. Pretty much, the scam and the work that you turn in yields all that money that gets wired out, they keep it. *You give a little to your criminal ring. You give a little to your money mule organization that actually picks up the money*, but most of that money they get to keep. You take a criminal ring of about 30 individuals and 3.2 million, that's, that's a lot among those guys. I mean that is a nice pot of cash I think they can do some work with, or maybe they use it to buy their next tool. It's amazing to learn how sophisticated these rings are getting. We have people here going to graduate school. They are spending two years of their lives to get a degree. These guys can get up to speed in about three, four months and really create some amazing attacks.

Suzanne: So there is the organizational aspect of it then, and then there is the personal aspect of it. Using myself as an example, one of the things I've become very conscious of, and our IT shop

does a great job of, is filtering. When we first started with email clients and we were trying to protect ourselves, I was probably putting 30 percent of my mail was going into the junk folder. Now, I would say maybe three, four emails a week is all I have to deal with individually. I do things like check the actual email address. I got one recently that said, *This is American Express call us about your account, blah, blah, blah blah*. The address is some weird email address that has nothing to do with American Express. That is a really easy one to pick up on.

If somebody sends me something where they are asking for anything that is private information or semi-public information, I'll check on it. We have an email alias called *suspicious*, which I love that name, check with them. *Is this something you have seen? Should I pay attention*? Every once in a while, it is somebody for real, and I do have to pay attention to it. So, there is productivity loss. I agree with that, but the, the volume isn't that high. What are some of the other things that people should just on a routine basis be doing just to make sure that you don't get caught in, in one of these scams? I knew it was out there, but this is news to me too that this is such a big deal in the business world.

Anne: Well, again, a really good question because, and I keep saying this, it's amazing the companies that are falling for these things and the amounts of money again they are taking. So, I would like to address that in two parts. One of the things that always bothers me is the empathy part that you have for the people that fall into these traps, get hit with these scams when they are successful. I always look at that as the motivation for, *How do we empower these users*? Again, don't make them the last line of defense. But if you are going to make them the last line of defense, give them tools which they can use to prevent it from happening. I will talk about both sides of that. The first part is what can the companies and organizations do. Well, obviously, patching is always huge. So, applying the software patches, looking at the vendor bulletins...

Suzanne: Staying up to date.

Anne: Staying up to date. Believe it or not, there are a lot of things you could do just with the tools that you already have. So, Office 365, right now, has been recently hit with these issues. The link in the email that said, *Hey, your account was flagged. Click here. We are going to have to close that account.* And then, *Click here in which to reauthenticate and sign in again*, so they get your credentials. Finding out that Microsoft is now creating ways in which to prevent that happening is what I am talking about with the regard to vendor bulletins.

One of the companies that I was working with on another project because the spear-phishing was so bad, the campaigns. That is what this SOC [security operations center] was dealing with. There were four people in that security operations center. All four of them told me, *Yes, what we are dealing with the most aren't the viruses, isn't the malware or the ransomware. It's the spear-phishing campaigns.* And spear-phishing campaigns are obviously connected to what these

attacks are. The idea that to thwart them because this was a really very rich company in an industry that was pretty important and scary. I won't say the name. They actually created an affordance for the user to say, *Hey, I think this is spear-phishing*. They could click on a button in their email client and report it. So, empowering your users...

Suzanne: Make it easy for them instead of hard for them.

Anne: Make it easy for them. In fact, if it was a true spear-phishing campaign that was sweeping through the company, not only could they have early detection, especially if one of the network appliances didn't pick up on it. They would then reward that specific user who reported it first. There was a $5,000 incentive. They would get paid $5,000 for identifying this campaign, which tells you a little bit about the revenue of that company.

Suzanne: That makes people more vigilant.

Anne: Right, and aware and proactive. So that is a UI affordance. There are other things you could do with UI. You could color code all of your internal mail versus your external mail. You could have rules that say…Maybe a Cyrillic font has been used in which to put the domain apple.com, but instead of apple, it's *A-Q-Q-L-E*, and they specifically use a different font so that it looks like it's *A-P-P-L-E*. Make sure that those rules for undefined characters, or this isn't a real domain, or the idea of, *This is email you've never gotten from this user before, ever. Make sure that it's legit*.

Suzanne: To create warnings for the user.

Anne: Yes. Also make them simple. There is a whole area here, CyLab, Dr. Lorrie Cranor, working in the areas of privacy, security, and usability. We really need to emphasize addressing ways in which users can easily be proactive about this instead of falling for these campaigns. I would also add that, not just the color coding, but there are tools out there. You can use DMARC. You can use SPF [Sender Policy Framework]. There are a lot of things that are already on the way to really addressing these types of risks, but they are not necessarily implemented yet. It is going that way, but we are always playing catch up. We are always finding ways in which to respond. We really need to, on that spectrum, we need to move to the proactive instead of the response by creating ways for people to be more aware and able to take action.

Suzanne: I think this is a great podcast for people to build awareness, especially people like me that had no idea how big this was. I knew it happened, but the size of it is something that I think a lot of us…unless we are in one of those companies, we are not going to hear until long after the fact about how much money is involved in all these things. Taking that, *How do we become more proactive?* What is the direction of the research that you are working in to kind of help us to deal with these kinds of compromises in a more proactive way?

Anne: A lot of this information stems from some really good training that myself and Larry Rogers and John Dayton did, we helped to build training. The FBI was our sponsor on creating ways to address your standard cybersecurity crimes. There was a level-one training that was around digital harassment, online fraud, identity theft, child enticement. We created courses for law enforcement to know how to address these types of crimes. Now, the FBI sponsored it, but they really wanted it to be for the 750,000 sworn police officers out there. By level one, I mean *where the person is the target*. That was great training. It is still being used. What we did then, we were moving to level two. That particular training, the goal there was to talk about business email compromise, talk about it more at the network level rather than the individual level. The plan—we didn't get to, to do all of them, yet. Hopefully, that'll change—the plan was to teach first business email compromise. That was picked by the FBI because it was becoming such a common threat. I mean ransomware was on the rise, but it hadn't toppled BEC [business email compromise] yet.

We were moving in that direction to create this training. What I found so interesting was not just teaching law enforcement on how to deal with these crimes and how to investigate them and identify the subject that was actually conducting them. Also then, my perspective was, *How do we handle and empower and basically give tools to the individual that is being attacked?*

I had a lot of empathy interviewing both the investigators on these cases and then, in some instances, actually talking to the users. That is the thing that I really tried to drive home working with students, working with coworkers, understanding that the colleagues might not have this view into what has happened with a particular attack, but the idea of there is a victim. That victim isn't just the company. The victim is the user. This has enormous impact. This impact not just because of the privacy breaches, say, with Equifax or with…

Suzanne: OPM [Office of Personnel Management].

Anne: Yes. I mean, there's a lot. In 2018, they just keep climbing. There's more and more. Marriott. I got hit with the Target one years ago. I got hit with Marriott just last year. I mean, credit cards are useless, credit card numbers. Basically, the credit card companies have fought back. They will call you. I was in San Francisco for RSA, and I couldn't check into my hotel for about two hours because I had made a couple of purchases. My credit card company called me and said, *Are you traveling? We're not going to release this until you confirm*. I was like, *I want to go to sleep in a hotel*. But I'm glad. So, credit card companies have caught up. They don't want your credit card numbers so much, now they want your credentials. Why they want your credentials is because you might use that for your bank. You might use that at work. You might use that for your social media accounts. We have to make sure that users are aware how risky that is. Use different passwords or use a password manager to prevent that from happening.

When talking to the individuals that are at the tip of the spear with regard to these attacks, they are not aware of this and the impact that it has. They have less confidence in their financial information and where it's being stored. Some of them actually start to use the internet less. The idea that you'll lose your job. Because they are being tracked, there has even been uptick in suicidal thoughts kind of stuff. That is the part that I tend to look at because I wish to create affordances for users to be aware, not just through the organizational training and awareness but aware more broadly. That is getting to this data privacy survival guide. The idea that the same rules that you apply at work, you should apply in your personal life.

Suzanne: When it comes to data privacy, the questions on Facebook about, *Answer these 20 questions with me*. I tell people that put those things up, private message them, and say, *Do you really want to do that*? Because you are giving away information that somebody could use against you, because it's not just us. It's not just us in the room anymore. Things like, I have a friend who was posting pictures of his vacation. It's like, *Oh great. You just told everybody that you're out of town*.

Anne: Let's go break into your house and steal all your stuff. Yes.

Suzanne: All these things that, I don't like knowing these things.

Anne: My point here is that I'm guilty of all of this, too. It wasn't until one of those quizzes that I suddenly became worried for all the people that were getting in on this and liking it. Right away—not that you weren't being respectful of their privacy—but I felt the need to respond to it publicly as well because then you might reach all the people that are paying attention as well as the private messaging. I say do both. My intent is to not embarrass those individuals. It is more like a PSA saying, *Hey guys, if you're tracking this, just know these are your security questions, and you don't want to do this*. Think about these things before you might respond and/or even forward. Maybe even just that, not only gets them thinking about their, their information they have on Facebook or their engagement. But then it, hopefully, spreads to the other social media platforms that they are on as well as think about that at work, too. You are basically making it pervasive.

In many ways, I think it is important to understand social media, it's your digital self. It's not your personal self. The same things that apply to you at work, almost all those same rules should apply to you on your social media. The idea that one of the ways in which these attackers conduct the BEC is they will use PIPL. So, that's P-I-P-L. That service tells information about you [that is] pretty frightening: where you lived, who your connections are, family, previous addresses. It also tells you all the social media applications that you are using.

Say they do have your credentials, your work credentials. They could then try that same technique on any of the other social media platforms you are on. Again, the idea that our data is out there, that it's compromised. That it has been aggregated and available on not just the dark web, by the way. There are publicly available data sets out there, OkCupid. It's unbelievable how many of the dating sites have been hacked. I mean you have your Ashley Madison. I mean 400 million users across those different dating applications, their credentials could potentially be out there. Their accounts have been compromised. We are talking about a lot of people. If you compare that data set with, say, a breach of some company, you are going to find some correlations.

Again, I want to plug some work from here at Carnegie Mellon. Professor Latanya Sweeney, she did a remarkable and wonderful amount of work with k-anonymity. Because of her Ph.D. research and when she was working on her thesis, she was able to identify an individual based on health records and voter registration logs. In comparing all the fields that were available from those two sets of data, she was able to figure out that you only need date of birth, gender, and ZIP Code, and you can pretty much identify anybody, just those three fields. Typically there are about 18 [fields] that you enter on any web app, any form. The idea that all of these records are now digitized. They are not necessarily on paper somewhere. They are available. If that hospital, Hollywood Presbyterian Hospital [Medical Center], they had a ransomware attack. They were held hostage for a week, couldn't take patients. The idea that those records were compromised. You go after a group of people that would go to Hollywood Presbyterian Hospital and then, you start looking at the social media accounts of the individuals in that ZIP Code, again, you might find some really wealthy material.

Suzanne: Lucrative targets.

Ann: In tying this back all into BEC, I'm hoping to make it very clear that the contrast between the criteria of say a flight from Lagos, Nigeria, to Houston, Texas, was the criteria then and the companies that were selected based on….

Suzanne: Which is kind of feeling really random.

Anne: A lot of the methods are the same. They are consistent. What is happening is their research, their criteria. They were already working with these existing money mule organizations. That really hasn't changed. The method of picking up the money and getting it back to the ring, that isn't different. What is different is how they are selecting their targets, the multiple ways in which they are able to get access to the information, both publicly available and dark web social media mining, and the idea that, indeed, they are really getting good at it. I mean, they are on top of these vendor bulletins. They know that Office 365 had a vulnerability. They got up to speed remarkably fast, and that is what we are dealing with. I really want to

emphasize the idea of our data is out there. It is available, and we need to dial it back. Make use of the security.

Suzanne: I've got a bunch of things going in my head, right now. A list of things in my head. It's like, *Oh, I need to fix this, I need to fix this, I need to*...which is what you want for all our listeners. I think dialing it back is actually one of the messages. If you think that you can't be compromised, you are wrong. So think about what you do and how much risk you're willing to take. That's, I think the, the lure of all these applications that let us share and let us do things. I love a lot of the social media stuff. I have nieces and nephews that I don't get to visit very often, and I get to keep up with them. I love that. I love seeing my nephew in a swim meet and things like that, but I have to think about by engaging with that, I get into all these other things on the periphery, and they are not as innocent. There are people out there that will use my data if I let them. This is really the 2019 version of *caveat emptor*: *beware of not just what you are buying, but what you're giving* is really what I'm hearing.

Anne: You are giving access to yourself, and you are increasing your chances of being a victim.

Suzanne: Okay. Well, on that wonderful positive note…. Some of our podcasts like this are very cautionary, and this is one of them. Don't become a victim. Do your own due diligence. Even if your company doesn't happen to be one of the ones that is very proactive, you can be proactive yourself. You have got the blog post that you just put up. We have got the data privacy guide. That's not just for companies to read. Individuals can use that as well. So we're trying to make these kind of resources available to people.

I want to thank you for your work in this area, and I really want to thank you for being sympathetic to those…. They are victims. I can just imagine the woman or man who did the $3.2 million wire transfer and then found out that it was a fake. I would be devastated. That is exactly the word she used, and it wasn't intentional, wasn't her fault. We have to protect against that in the future, and we have to make it less lucrative for these…. This, in my mind, all of the cybercrime, the theme for me is make them have to work harder for it. There's a point at which if they have to work too hard for it, they're going to say, *It's not worth it*. So that's what we have to do.

Anne: You're summing this up incredibly well, but the idea is there is still a user at the end of this. The idea that their privacy has been invaded in order to conduct these scams, it makes the physical self feel vulnerable, as well. Truly, the idea that I want to come across is, empower your users. Don't make them the last line of defense, but if you do, make sure that they have affordances with which to fight back. Essentially, inform them of the idea that your data is out there. Don't let it be used against you. Up that level of awareness, and give them sort of a rule to go by, because we don't have the cognitive load to keep every single company breach in our

heads. But if you give them best practices to prevent this from happening to you and protect yourself, that will work. Let's be reasonable, here. It's not going to be memorizing NIST 800-53 rev five.

Suzanne: Well, I want to thank you, again, for joining us today. I hope that our viewers will look at some of the resources that we will post along with this transcript. As always, we thank you for listening, look forward to people protecting their data.

Thank you for joining us. Links to resources mentioned in this podcast are available in our transcript. This podcast is available on the SEI website at sei.cmu.edu/podcasts, and on Carnegie Mellon University's iTunes U site and the SEI's YouTube channel. As always, if you have any questions, please don't hesitate to email us at info@sei.cmu.edu. Thank you.