Barclay Damon Live Presents *Cyber Sip™*
Episode 42: "Social Engineering: The People Problem of Cybersecurity," With Arun Vishwanath

Speakers: **Kevin Szczepanski**, Barclay Damon,
and **Arun Vishwanath**, Avant Research Group

[Kevin Szczepanski]: Hey, everyone, this is a *Barclay Damon Live* broadcast of the *Cyber Sip*. Practical talk about cybersecurity. I'm your host, Kevin Szczepanski. Let's talk.

[Kevin]: Welcome back, everyone. Arun Vishwanath is an alumnus of the Berkman Klein Center at Harvard University, formerly a tenured associate professor at the University of Buffalo. And today he is the chief technology officer at Avant Research Group, which is a Buffalo-based cybersecurity research and advisory firm where Arun consults both with major corporations and government agencies on issues ranging from cybersecurity to consumer protection. He is also the author of many books and publications, including this one from MIT Press, The Weakest Link: How to Diagnose, Detect, and Defend Users From Phishing. Arun, you are one of the great cybersecurity thought leaders, and I'm so glad to have you on Cyber Sip.

[Arun Vishwanath]: Hey, Kevin, it's great to be here.

[Kevin]: Thank you so much. Well, today I want to talk about social engineering and borrow from one of your key phrases, which is "the people problem" of cybersecurity. That's really what it is. Let's dive right in. But first, let's get a working definition of "social engineering fraud." What is it?

[Arun]: Right. So, when we generally talk of social engineering, we're talking about attacks where the hackers are compromising users, right? So they're using any means, and there's a lot of different means out there. Right? So today we get pretexting emails, we get spear phishing emails. They're different, right? One just has text, the other has a malware payload of some sort. You get text messages, you get phone calls, you get social media attacks. You may even get something as simple as a USB drop off for the people who still use USB sticks. It could be Wi-Fi snooping, right? Or Wi-Fi sniffing, depending on how you want to use it. You create a fake Wi-Fi account, people log into it, you start extracting data from it. All of these are different types of social engineering attacks, and there's a whole gamut of them. Every one of them targets the user directly using a technology as an indirect conduit. So that's your working definition of social engineering. And if you look at the last 25-plus years now, they have just exploded, right? As more devices have come in, iCloud, different cloud services, IOT devices, you know, everything from wearables to the technology that we carry... iPads and more and more... everything is now connected, which means the number of conduits to indirectly get access to an individual, and then to the individual, their organizations, their networks, and everything that's held by that corporation is...basically what we talk about when we talk about social engineering. So it's a pretty big umbrella of attacks.

[Kevin]: So I suppose, I mean, it's expanding because it works so well. The question I have for you, that I wanted to get your thoughts on is: why does it work so well? Because on one hand, if you think about it logically, we know they're out there. We know they're attacking us all the time. You would think that over time we—employees, managers, users—would become more adept at spotting spear phishing, smishing, the various attacks. But we're not. I feel like we're almost getting worse. Why? Why are these... why is this vector so successful?

[Arun]: Right. And it’s a great question, Kevin. The fundamental reason this factor is so successful is because we have never addressed why people fall for it. Right. The presumption, you know, you exact same presumption that everybody does, which is, hey, I know about it. We’re more aware of it. But clearly what the evidence shows already is that awareness doesn’t equate to knowing what to do about it. Awareness doesn’t equate cognizance, right. So knowing that there’s a tornado coming doesn’t mean you know how to deal with it. Mm hmm. There’s a flip side to this. Right. Awareness is something, you know, as a as a cognitive scientist. Right. It happens with the cognitive level. That is, you know, you recognize something or your, you know, your mental space. You get to know of it. But there’s also behavior. Right. Sometimes people just react. They don’t even think about it. A lot of our behaviors are reactive habits of doing things. So a lot of these things are happening because of poor habits or rituals, poor ways of using technology. Awareness is not the only problem anymore. It’s all these other things that we have not looked at. And unfortunately, what’s happened is we have been addressing the problem with the assumption that we know what the problem is. It’s like, you know, I use this analogy a lot. It’s like going to the doctor and he or she just kind of walk into the office and throw a pill at you and say, go take it, Kevin, you’re going to be good in a couple of days. And then you’re like, hey, you know, I come back, I’m sick. They give you some more of it. And you keep going through this, getting sicker and sicker and sicker, and then they start blaming you for it. And that’s what is the people problem. The people problem is blaming the user because... what did the doctor not do? They didn’t diagnose the user? and diagnose what the problem was? So we have been doing this now for almost 10 or 15 years, even as the threats have expanded and even though the threats have expanded, to put this in context, the quality of the threats have not. So, you know, if you really look at social engineering, the original, if you want to call it, the first kind of real attacks that stopped coming happened in 1998 in the AOL community. I talk about this in my book, “The Weakest Link.” In the AOL community you have the first spear phishing attacks where they basically hack passwords and take the passwords and use the user’s identity. Those same attacks still continue. Business email compromise. So the FBI’s IC3, you know, ranks them at around, you know, 30 to 40% of all social engineering attacks. So businesses, you know, compromises, they’re worth tens of billions of dollars. They haven’t changed. The same vector is being used because we’ve never addressed the underlying reasons why those vectors work. Right. So these guys don’t need to get more sophisticated, as much as we need to get more adept at explaining to the user or addressing the underlying cause. So the treatment has got to match the user needs. That’s something we’ve never done.

[Kevin]: So let’s talk about that. What is the underlying cause? You mentioned earlier, cognition versus behavior. So if I were guessing, I’d say our behavior doesn’t match our cognitive awareness of the social engineering threat. There’s some gap there. Am I on to something or is it something else?

[Arun]: But before we even go there, right. Let’s look at how we’ve been addressing this for now. Let’s see what we have been doing for like a decade now. Right. There’s a massive... there’s a multibillion-dollar industry out there of basically training people.

[Kevin]: Yes.

[Arun]: And what we’ve been training people. So today, training is like, you know, I look back at the 1930s when sales tax was introduced in I think it was Kentucky, that interview sales tax. The first state to do it. And it’s hard to think of a time where there was no sales tax.

[Kevin]: Yes, it is.

[Arun]: Now, it’s hard to think of a time where there isn’t sales tax. It’s like, oh my God, we have to pay it. And training is the same way today. Every employee gets trained, sometimes repeatedly gets trained, or you have to get trained or you have to get certified. What are we training them on? Right. So the gold standard of training right now is either you do some classroom type training, online training, or the so-called gold standard is we send them a phishing pen test. Right. And we say, hey, you know, did you fall for it? And if Kevin fell for it or everyone fell for it, we’re like, okay, now we’re going to tell you why you fell for it. We keep doing this and that data is your cyber risk metric. So basically, if you really think about what organizations are doing, insurers are doing is they're taking that data and they're using that as a metric of how ready is Kevin or how ready. And I have... a since we were in Buffalo, I have this analogy even in my book. In fact, I talk about this. That is very similar to saying that the drivers in Buffalo are among the most dangerous drivers in New York State. Why do I say that? You look at the 198, you know, the Scajaquada has three times the number of accidents, especially, you know, if you look at the Scajaquada on your Main Street in Kensington, those exists that are there on the 90th the Humboldt, you can see an accident like I bet you every day you go by, I drive by that street.

[Kevin]: But I saw a very there was a very severe one yesterday afternoon and they're not rare, they happen a lot. Yeah.

[Arun]: All the time. Right. And I think a lot of people don't realize this that that the accident rate on just those two or three intersections is three times that of the state average on any New York state road. Out on top of that you take another metric. A lot of people in Buffalo probably don't know this but you know, the seatbelt was invented in Buffalo. Right. So we have a record of needing safety. We have a record of poor safety. Could we just say, hey, you know what? We have a lot of accidents. So Buffalo has got to be full of bad drivers.

[Kevin]: Or we'd say to ourselves, well, we have these safety issues, so we're going to make sure that we tell everyone on the road what the best practices are. We're going to train semi-regularly. These are the best practices. This is what you need to do. You need to wear your seatbelt, you need to look around you, you need to signal a lane change, and then we're done. And I suppose the problem with that is that you're not ultimately changing....

[Arun]: Passenger that would cause. Right, exactly. And if you know the street I'm talking about right at the corner of what is it, Humboldt and Main and just after Sister's Hospital. Yes, that's right. There are like seven or eight lanes that come in. They keep changing it. New York State has been trying to figure out what to do with that intersection because it was never originally meant to be there. The point of that analogy is that the problem is not the driver alone in that particular case. The problem is just the signage and the streets. So you can't always blame a driver because if you're not from New York or from Buffalo and you're not driving those roads all the time, you don't know where you're coming from or which side to even look at. So sometimes it's not the driver, but other times, I mean, you know, it's motorcycle season right now in Buffalo, the Scajaquada, you know, motorbikes go off all the time. There are accidents, I'm already reading a lot of fatalities on the Scajaquada. Yes. Sometimes it's the driver, sometimes it's the vehicle, sometimes it's the street. Sometimes it's a combination and an interaction between those things. Now, this is important, right? Because when it comes to cyber, we very quickly go and say, while it's the user or it's the lack of awareness.

[Kevin]: Mm hmm.

[Arun]: And it's neither. Sometimes it's the user, sometimes it's the way the technology has been set up for them. Sometimes it's something within the user, you know, what are those things? Right? So my research—and I spent 20 years as an academic social scientist, you know, replicating—and this was before spearfishing and social engineering where popular topics... I was basically creating these attacks that I found online, that I found in the media, and I would come and replicate those on students. And then within organizations that volunteered, within government agencies. And we recognized that there were only a few things that people... that could explain quite cogently what was going on. And we identified these reasons. And those reasons are about five reasons. All right. And it's a combination of those reasons that cause, in this particular case, an accident, an accident being you fall for a social engineering attack. Right. And so we know what those are. So what are those? Right. So they're cognitive factors. So cognitive factors being there are certain mental factors. And then there are behavioral factors. Okay. So give you an example of some of the cognitive factors. You know, we do this in a survey. We ask people, what do you think is more secure, a PDF document or Word document? What do you think the answer to that is, Kevin? What do you think?

[Kevin]: What do I think is more secure? If I were guessing, I would say it's a PDF document.

[Arun]: Right. And why did you say that? You're right. That's what everybody says. I... the vast majority of the people globally say exactly that. Why did you say that?

[Kevin]: And the reason I said it is because it is... it's more secure. Because it is less amenable to change or manipulation. That's my assumption.

[Arun]: Exactly...

[Kevin]: ... Than a Word document.

[Arun]: Document. And it's a very valid assumption, however. And that's the assumption 80% of the people in surveys have done all over the world have said, okay, so you're not unique, you're great company. But what's the fact here? What is any of your manipulation got to do with the security of a document? For me to put a backdoor in a document? I don't care.

[Kevin]: What does... it doesn't matter what I am able to do.

[Arun]: Exactly right. But you did exactly what people do, which is we take our model of reality and we apply it to a technology and no one ever corrects us. So we use that to govern the way.... So if I send you a PDF an attack a spear phishing attack, and this is where a lot of the early spear phishing attacks used to PDF documents, because they knew by trial and error that people opened them and they clicked on them because they said, hey, you know what can go wrong? And how many such ideas that you hold in your mind and you formed it without really understanding why. So there are many of them. So I'll give you another example. Yes, lots more secure a text. You know, if I text you a text message or a Facebook Messenger message, what's more secure? Well, what's not like Facebook messenger, WhatsApp? Pick any one of them.

[Kevin]: So now I'm going to change my thought process. My thought process is now oriented toward what system I think has more built-in security.

[Arun]: Right.

[Kevin]: So... but I'd be guessing, frankly. I would say yeah, I would say that the text message is more secure just because there's a phone connection. And I'm assuming without knowing that the security protocols are better than the protocols in some of those online platforms.

[Arun]: That's right. And you're going to say, well, and text messages cannot be edited the same way WhatsApp messages can. That's part of it. If I throw Facebook Messenger as the term everybody dislikes Facebook, right? Facebook is like, you know, public enemy number one right now.

[Kevin]: Right.

[Arun]: So would I trust Facebook Messenger to be more secure or text messaging to be more secure? And I've done this exact same question in service all over the world. And you're exactly right in the answer, but you're exactly wrong in your assumption. Right?

[Kevin]: Right. Right.

[Arun]: Text is actually the least secure of them. It's not even encrypted. It is so easy to hack a person's text message. Text message. Remember that? Because cell networks were built on and we don't talk about technology often, but it is incredibly easy to intercept a text message...you could do it, you know, in minutes. Whereas Facebook Messenger is end-to-end encrypted. Believe it or not. So WhatsApp messenger is end-to-end encrypted. Believe it or not, even Facebook at least claims that they can't decrypt it. Right. So intercepting it when it's encrypted, end-to-end is actually very hard. Now, again, you're not wrong in the way you're thinking, but you're flawed in your assumption of the risk of what you do. And these are just simple, basic behaviors.

[Kevin]: Right? No, it reminds me. Oh, I'm sorry to interrupt. I just wanted to share with you. It reminds me of an answer that former Defense Secretary Donald Rumsfeld gave at a press conference. When a reporter asked him a question, he said, you have begun with an illogical premise and proceeded perfectly logically to an incorrect conclusion.

[Arun]: That's a great way to put it.

[Kevin]: That's what we're doing.

[Arun]: I'm going to use that in one of my talks. That's a good one. But isn't it? Isn't it? But this is important, right? So we carry such ideas and these ideas are not just carried in our minds, but they are used to govern behavior. Right. So. So ideas are very powerful because intuitively, you're like, Oh, I got a text message that I should be fine, or I'm just going to text him or, Oh, here's a PDF and there are many more. Okay. So there's a handful of there is about 15 of them that we have identified as being very powerful determinants of how much scrutiny you're going to give to something that comes in an email or in a message.

[Kevin]: Mm hmm.

[Arun]: And so we call these things your cyber risk beliefs. So these are beliefs you hold and we all hold them, and they're global because of the nature of technology. And this is the powerful part of this... because of the nature of global technology, these beliefs are carried by people everywhere. Right. Text messaging is everywhere. Facebook Messenger is everywhere, just like Amazon's everywhere. So attacks can go everywhere and can come from anywhere. And you can take advantage of people anywhere and everywhere. This is why these attacks are all growing in scale, not necessarily in scope, but in scale, because we have never addressed the fundamental lack in risk beliefs and individuals that do lack it. Now, not everybody lacks it. Some people don't.

[Kevin]: Sure. But not enough. Not enough people have them.

[Arun]: Exactly. What we want to do. So this is the diagnostic approach, right? The diagnostic approach is evidence-based. So what we say is in the approach, in my book, we do a diagnosis. What we do is we do a pen test and a survey. It's a two-question survey. It's actually a very easy thing to do. But we're able to quickly identify, you know, hey, what are Kevin's shortfalls, like is he lacking risk beliefs and which ones are shortfalls? Has he got a bad habit? Now may have a different reason than you. And that becomes very significant from a correction point of view. Right. Look, not everybody who has an accident on that 198 has an accident because they didn't see the signage. Some of them may have poor eyesight. And we need to give corrective lenses to them. Now, giving you and I corrective lenses is going to be a waste of public resources. Right. So we do that in medicine. We do that in accidents. Well, we don't do that in cyber, which every one of us uses. Right.

[Kevin]: So in cyber. So, to sort of draw this analogy, which I think is invaluable, if we train everyone driving on the 190 to make sure that they fasten their seatbelts. Yeah. But we know empirically that the absence of a seatbelt is not what's causing the majority of the accidents or even most of the accidents. We're not...our training will be utterly ineffective at reducing the risk of an accident. The same with cybersecurity. So if I get a survey and I'm assuming this without knowing. Correct me if I'm wrong, but if I get a survey and, right, I have some incorrect assumptions about the security of certain systems and you tend to look quickly and click on apps and links without question. If you and I go through the same training, unless it includes both.

[Arun]: Right.

[Kevin]: We're not going to hit at every individual's vulnerability.

[Arun]: So one, is that right? And the second problem is, how much time are we wasting doing this? The third issue—and I've done this in companies, in different parts of the country. I'll be wasting your time and you'll zone off. The number of people who zone out of a training today. There's training fatigue in Washington, D.C. If you're in the federal government right now where your mandated training, you're tired of it. You're like, Jesus Christ, I got it again and again and again. And then remember, people game it. It gets worse, right? You know, I have this, you know, I do these pen tests where the manager basically tells everybody, Hey, there's a pen test coming, or the supervisors tell everybody, Hey, did you see that? That was a pen test. Mm hmm. Like, good at guessing it. Which means your cyber risk metrics are now flawed. Right. Because you're using the test to say, well, this is the pulse of my company. Well, that's not the pulse of your company. That was to game the pulse of your company. Right. Which is why when I go and do a test, I tell them, Well, wait a minute. You clear the deck. Don't tell anyone I'm doing it and I'll do it my way. And I've done this in companies where they would have less than a 1% clickthrough on up on pen test. Think of not having a single incident and suddenly I'll do it and they'll be 25% clickthrough, and they'll be like, we're going to shut this test down because now our auditors are going to get to know all of this. Right.

[Kevin]: What changed between the company's pen test and yours?

[Arun]: People get... people figured it out. See, people know how...Here's what changes first, how are these pen tests created? Right. So my book, I talk about this. You know, we have not just I just don't want to talk about the book per se, but I've developed a metric, a methodology to develop a pen test. So part of the problem is, what are these pen tests? How does the IT department pull out 24 to 30 pen tests a year? They just make it up. It's just basically going online and saying, hey, you know, here's an attack that just happened. Let's just replicate it.

[Kevin]: Let's replicate it.

[Arun]: You replicate it? What if people already knew about it?

[Kevin]: Then you're going to have a factor between the... what is the actual percentage and the actual.

[Arun]: Which you're going to.

[Kevin]: You're going to overstate. You're going to....

[Arun]: Or the flip side of it. What if a test is too good? What if I create a test that takes your first name and last name, creates an email account and sends it? Is that a valid test?

[Kevin]: No. Well, it's.

[Arun]: Or is it just me impersonating you. Like, at what point did the test show good that everybody's going to fall, right? The problem here is there seems to be no science on it, and that's not true. The science is there. It is that it's not being applied. And this is where I do it in my book, I talk about how do you develop an appropriate test? That's not too hard. That's not too difficult, that's not too easy. That's not just replicating someone else's work. And what we did to develop that is we looked at over 20,000 different attacks over time, that were done with different by different companies. And we worked backwards to see, okay, what was it in the attacks that were working? And we identified basically three factors that needed to be there. And then we actually... you could become a great hacker if you read that chapter because it basically teaches you how to create a successful pen test. Basically, how to create....

[Kevin]: Are the factors.

[Arun]: So there are basically three major vertices to this right. It's called a V, trial. So basically the way you try it consists of three vertices, right? So we look at, you know, there are three things that every phishing email has got to have that makes it successful. One is, you know, it's got what is called "credibility cues, these are thing that attract your attention, your eye's attention, but that appear very credible. Like it's getting an Amazon logo, for instance. Right. So there's one, there's a lot more science to that. So I'm just giving you the broad CliffsNotes version of this. The second vertice is, is what it's called is customizable. Right. There are certain elements of emails and messages that you expect will change.

[Kevin]: Mm hmm.

[Arun]: Okay. The Internet is full of them. So I'll give you an example. If you're ever sent... if you ever use Google documents, for instance, and you send someone a Google document sheet to share if they ever try to click on that email in it, that email will be not the person's email. It'll just be some random number that email, that Google trust account you're used to mentally adjusting for and saying eh, it's okay. So I take advantage of that as a hacker because I know what things you will ignore. And the third thing is routines, right? So if your routine is to check emails a certain way or to expect something on a certain time like tax season, people expect some stuff from the IRS, right?

[Kevin]: The holiday...

[Arun]: ...lawyer follow certain cycles. There are quarterlies that people are filing If you can capture those cycles that creates compatibility with how you're thinking. Right. So there are these various elements that we put together. And when you create it, in fact, right now, you know, as we talk, we have an attack that we're doing on students work and we're doing... we're comparing an AI-based attack, versus the attack using the V... What we're doing exactly that. Right. And there's another element to this, whereas which is we don't just develop a phishing pen test, we measure its baseline. And in my book, I detail how we do that. So in other words, we develop a test and we have a numerical score of how what we're going to expect if we hit the market with it. All right. And there's a methodology for that and it's all in the book, and then we then test it. So now we have a score, a baseline score. So let's say the score, it's a score from 0 to 100. Let's say that score is... we're expecting a score of 60 and then we measure to see, you know, what did Kevin rate it as, is Kevin saying this is an 80, which means, you know, there's a 20% gap, right? Which is where he should be, then we know where and then we look to diagnose what the reasons are. So so that's kind of like a in a nutshell, what we do, which is a diagnostic approach, right? And it's no different than how American medical science works, right? When you go to check your blood pressure. Right. There's a blood pressure cuff that is put on you. But it's not just about blood pressure cuff that's put on. It's got to be put a certain way. There's a science to it, and there are numbers against which it's measured, right? There is a baseline, right? If you didn't have the baseline, you would.

[Kevin]: All right.

[Arun]: It's all meaningless. It's just an exercise in numbers.

[Kevin]: You might know. And this is another great metaphor. You might know if it's terribly high that that's a problem, or if it's terribly low, that's a problem. But for everyone else in between, without that metric you're talking about, the testing is meaningless, right?

[Arun]: And right now all we have is a pass/fail metric. All we have is number of people who fell for a phishing test, number of people who passed it. That's it. That's like saying, well, how many accidents happened on the 198. Well, a lot. It doesn't suffice...

[Kevin]: Because we're not addressing the underlying behavior. And unless you do that.

[Arun]: Right, we're not just the behavior, the underlying causes. And it could be cognitive or behavior. Yes. Remember that, right? It's the action or the thought. So it's just as important to know, going back to the 198 analogy, it's just as important to know why some people had an accident and why some people did not. So that's a part we often miss. Like, why are all of us not having those accidents? What are we doing differently in our driving style? What are we doing differently in how we're thinking and orienting to the problem, to that space? The moment... I actually avoid that completely, like I go down Parkside, I try to avoid it completely because it's so yeah, there are certain things people are doing in their mind. They've already rectified it and created a new ritual. That becomes important.

[Kevin]: So how then do we convert this research and this methodology into a training program that works. Because it sounds like what we're saying now is that what we have is it's better than what we had before. Maybe because something is better than nothing, but it's not ultimately effective because we're still seeing the same problems repeat themselves and.

[Arun]: It's never going to be effective. Right? I mean, because we have never addressed the underlying problem. And there's a reason for it, Right? A big reason for it is that training right now is not a solution. Training is a product.

[Kevin]: Yes, exactly.

[Arun]: And the problem with that is training leads to more training. Justification for training.

[Kevin]: Yes. How that it's funny how that happens.

[Arun]: And it's so obvious, isn't it? It's kind of like it's glaring at us, right? So every time the training is done, they tell you how much more training you need.

[Kevin]: Well, in.

[Arun]: The doctor diagnoses you to need them, need him or her. Yes. You need me.

[Kevin]: The regulators are buying into it, right, by requiring more regular and standardized training?

[Arun]: Yes. Is there a surprise there? In fact, you know, in one of my articles I talk about this, the amount of lobbying money that went into it. And I'm not against it, but what I'm saying is, sure, you know, we got it. There are certain things where the free market doesn't do well, right? Astrology, mad science. You know, there are certain things homoeopathy, you know, I don't think you should leave that to the free market, cupping, you know, all that nonsense that comes out. You leave it to the free market, people get hurt. I think, you know, security is something I don't think security, education, security, training, we've left it to the free market. Nothing wrong with it. But the science on it is being ignored. The product has come before the solution. Right. So basically what happened—and I don't blame them. Okay. As a former academic, there's a good reason I'm a former academic because academia doesn't solve the problem either. Right. Academics can talk about a lot of things, but they're not the guys creating the solutions.

[Kevin]: No.

[Arun]: In fact, what they do is they just punt the problem to somebody else and you know, they're not going [hard to hear]. Vendors. I mean, they get—a I give them a lot of credit for putting money and capital and time and resources into it. The problem is that they're already committed to it. So now we're kind of asking them to go backwards and say, how do you inject science into this?

[Kevin]: Hmm? Is it too late? Is it too late, though?

[Arun]: I don't think it's ever too late. I think it's never too late. Right.

[Kevin]: Maybe it's just... for our audience. And forgive me for interrupting. The reason I ask is that my assumption is once a given vendor gets too far down the road, it becomes very difficult to back up and impose some scientific structure on the product, because the product is already created. The assumptions that led to its creation and purchase and replication have...They're already baked in.

[Arun]: That's true.

[Kevin]: So how how do you go about putting the brakes on? Go back to our car metaphor, putting the brakes on and imposing some sort of scientific method to the process.

[Arun]: Well that's been the hard push. Right. You know, there's this old saying, right. You can't pull a string uphill. And I've been pushing my string uphill, which is what we're trying to do, which is why I wrote the book, "The Weakest Link," because the idea was we have the science, but we haven't incorporated it because the vendors are too far entrenched in their products right now. And some of them, to their credit, are trying you know, the newer ones are now, you know, I'm working with some of them where they're trying to say, hey, can we do this differently? And I think we'll have to. I think either... if you go through the halls of Washington, DC, you know, everybody knows or everybody talks behind closed doors saying, well, training doesn't work. Everybody knows it, right? It's like the best kept secret in town is training doesn't work. But what do we do about it? Well, we can't do anything because we need a product and the product is what we can put it. So the problem is ideas are hard to show, products are easy to demonstrate.

[Kevin]: Yes.

[Arun]: And that's where we are, right? So I with my product, I'm... not product with my idea, with my concept of diagnosis, it works with existing training. So you don't have to change how you do things. You don't have to throw the entire, you know, vendor market out. You can inject it into it and improve it. Certainly work with what they're doing, not against it.

[Kevin]: So it's an easier fix if someone wants to implement it. But let's so let's start implementing it.

[Arun]: You know, I'm not saying no one is there are companies there are companies even in Europe and in Asia and in the United States who are way more open to it and are trying because they were also recognizing that, you know, the status quo does not work.

[Kevin]: Right. Is it a back-end solution, Arun? Or is it a front end? In other words, if ...just talk let's talk a little bit about in the time we have left, what is this look like and will it be something that I, as the testee would notice, or is it on the back end in the sense that we're using more prudent methods and diagnostics to really make this training tell us something that we can then use to change thoughts and behavior.

[Arun]: So you as the user would see it. In other words, you know, unlike... so currently, let me just put in perspective. You're right, current testing is basically we send you a pen test, you click on it. It's done. In the approach that that I have in "The Weakest Link. We send you the same test. The test for you looks the same. But the only difference is we send fewer tests. You don't send as many because we don't need that many. We are able to diagnose you with, you know, you don't need a blood pressure monitor every hour, right. Because we have a more accurate measure. And what we do after the test, though, is we do a short survey, we capture your thoughts. And that's something that that's a different part of that process. So we captured your thoughts more often, maybe once, maybe twice a year. And then we get to know exactly what's missing and where you've improved. So you can have pen tests throughout the year like people are doing. The two of them are going to be a little different. There's going to be a survey after that. That's all it is. As a user. That's all you see as the IT person, as the insurer. You get a ton of data, you get to see what's lacking and you get to see what's working. So if I do it, you know, at the end of the year, if I do it twice a year, but some companies would do it twice a year, beginning of the year, end of the year with a following a pen test, we do a survey, we're able to say, okay, you know what? What were we did didn't work or didn't work and why?

[Kevin]: So then how do you take that data or run and analyze it and use it to improve going forward?

[Arun]: So what the approach gives you is it gives each person a cyber risk index. So it nets out a score from 0 to 100 for every person who participated in it. And this is very easy, right? The higher the number, the higher your risk.

[Kevin]: Mm hmm.

[Arun]: Such a very simple index. An index tells you at a glance where that person stands compared to everybody in the organization, compared to an industry, compared to everybody in the nation, depending on how you want to aggregate it. It also gives you that metric with a level of granularity that explains the "why" behind the metric. So think of that zero 100 score, no different than a financial credit score. Now you have your credit score and the reasons this person has bad credit? That's the diagnostic part of the survey. So between the two things we can say, what's Kevin's risk? Where's this risk coming from? So now when I have those two pieces of information, if I need to solve the problem, I can. So I'll give you an example. Right? In some companies, what we did is we found that, you know, certain people, not everybody, they had really poor email habits, right? And what they were doing is they would show...so, poor email, habist, how do we solve poor human email habits. Right? What we did is we basically give them iPads and took them out of using, you know, large scale computing devices for accessing email. So the sandboxed, the problem, so you can continue to have your habits, but now it's restricted to a sandbox environment.

[Kevin]: Mhm.

[Arun]: Right. So it's a very simple way to fix the problem. So the next time the attack came in, most of these guys were very much way better at addressing it and dealing with it. And the ones who didn't, the risk was very low. So, so you see how novel the solutions are. The solutions don't always lead to more training like we do right now, which is, you know, what's the solution to you know, Kevin's problem, throw some more training. And the point of this, you know, cascade of training is at what point does it end and what point are you ready? If you ever ask any trainer, what's the end goal of this training? Like, what am I supposed to be a computer scientist by the end of it, right?

[Kevin]: No.

[Arun]: Because even a computer scientist, I can bet you and I've done this, can fall for a phishing email if I send it to them. Right, because. And what level of knowledge are we talking about here? Are we going to be like, you know, expert level? Because even they fall for it. And so knowledge and training is an end in of itself, whereas solutions like changing habits are unique. They don't need more training. It's a solution, it's an end-all fix. We fix the problem, we can move on.

[Kevin]: So in the moments we have left, let me pose this question to you. How do you convince an organization that it's already investing more than it ever has before in training? You know what? Everything you've been spending, it's fine as far as it goes, but it's really not getting you to where you need to be. You need to rethink and implement anew...a training and diagnostic analytical process. And it's going to put you in a much stronger position than you're in now. Right. But it will come at a cost. How do you make... I know it's an unfair question because we're all making....

[Arun]: I deal with every day.

[Kevin]: Yeah. How do you make the case that, look, this is something that, yes, it requires an additional investment, but it's a must. It's a must do.

[Arun]: Right. And the answer and the reason or the approach is basically a time and cost approach. Like what are you spending in man hours, in human hours in these tests? Are you willing to commit more time? And at what point does that stop? But you could do this next year and then the year after and then the year after? We spend a month on security awareness every year since 2004?

[Kevin]: Right.

[Arun]: Is awareness ever going to be enough? What is that level of awareness that we're talking...so as a company you can say, well, you know, I can spend all my time doing this, or a lot of our time doing this, or I can be smart about it and only do it to the people who need it. And I can save a ton of cost. I can save money, which is what it is. Security is a cost center.

[Kevin]: Sure.

[Arun]: And we're teaching you how you can save more money while ensuring that the enterprise is secure. Because right now what you're doing is you're throwing money at the problem and you're still not sure if you're secure. There's always that nagging feeling, did I do enough? Because I know it doesn't work right? You'll get me... if you ever ask an IT person. You know there's a ceiling effect on test. About 10% of the people always fall. And if you ask them why, they don't know. The number of emails I get from people saying, I don't know. I've tried everything. I don't know why it doesn't work. Well, I can tell you why we can get that 10% down to less than 1%, maybe even to none in some cases. So is it the peace of mind, the security, and the lower cost? Are you willing to get that? Be willing to trade peace of mind, security, and lower cost for a tick box? So you can tell the federal government that, hey, I got training done. What would you rather have. I think you'd want both, but ideally you'd want at least security, peace of mind, and reduced cost, and your employers will thank you for it. Because now they don't have to keep doing this over and over and over again and, you know, thought behind the IT person's back saying, here comes another test. And think about it, right? More tests you send, people change behaviors, they stop checking, email, productivity goes down, customer service quality goes down. We never measure those things, but they do matter.

[Kevin]: No, we don't.

[Arun]: Right. And ensure professions like... if you think about physicians, lawyers, you know, most lawyers I work with, at least, you know, the newer crop of them are the younger ones are very good with technology. The older generation was very bad with technology. So very dangerous with technology because, you know, you don't want to put anything in writing anyways. So, here's an easy target for bad guys, you know, and these are the groups that, you know, if we want to protect them better, but we have to right. Because by now everybody is ...something has been lost. Are we okay with that?

[Kevin]: So last thought before I let you go. If someone is listening to this and saying, okay, well, I got to an employee training program in place, but it sounds like it might not be as effective as it should be. Where do they go? Who do they talk to? Learn more about how to implement a more proactive diagnostic analytical system?

[Arun]: Well, look, there's two things you could do. One is you could email me. Well, that's the easy approach. Or two for the price of a book, you can figure it out. That's right. I mean, "The Weakest Link" is available on Amazon. It's available on MIT Press. You know, the science is in it and it's written for the IT person. It's not written for an academic. I'm trying my best to put away my academic hat and write this so the person can take this and run with it. And remember, this is not just an American problem. This is a global problem, right, right. I mean, this book has resonated in Australia, has resonated in the UK. I have people in Singapore, have people all over the world who in France, used different parts of this book to actually make a difference in their companies and as vendors. And I think that's just the least we can do if we're really serious about it. And I think the security guys really are. I know many of them. I know they take that... their jobs are on the line. You know, this is what I didn't like about being an academic, which is you can talk and get away with it, whereas they have to put their job on the line. And I think, you know, as the world gets a little bit more fragmented, a little bit more dangerous, these attacks are going to become more meaningful, more... larger in size, more consequential. It's already there.

[Kevin]: Right? Well, Arun Vishwanath, the book is "The Weakest Link: How to Diagnose, Detect, and Defend Users from Phishing" from the MIT Press. Arun, thank you so much for joining us today on *Cyber Sip*. Enjoyed this conversation. Will you come back sometime soon? We've got many topics that we can cover and I look forward to it all.

[Arun]: Absolutely. It's a pleasure. Thank you so much. Thanks for having me. Look forward to it.

[Kevin]: Thank you. I appreciate it. And thanks to all of you for joining us for another episode of *Cyber Sip*. We're back soon with another episode of *Cyber Sip*.

[Kevin]: The *Cyber Sip* podcast is available on barclaydamon.com, YouTube, LinkedIn, Apple Podcasts, Spotify, and Google Podcasts. Like, follow, share, and continue to listen.

This material is for informational purposes only and does not constitute legal advice or legal opinion. No attorney-client relationship has been established or implied.

Barclay Damon Live *podcast transcripts and captions are automatically generated through artificial intelligence, and the texts may not have been thoroughly reviewed. The authoritative record of* Barclay Damon Live *programming is the audio file.*

Thanks for listening.