CTL-CISO-Todd-Smith

Mon, Apr 27, 2026 5:40PM 16:09

SUMMARY KEYWORDS

AI security, shadow AI, IT problem, security problem, data leakage, regulatory breaches, network visibility, API management, employee training, NHS, AI defense, Skynet, security protocols, threat intelligence, financial services.

SPEAKERS

Jo Peterson, Todd Smith

J **Jo Peterson** 00:00

Jo, Hey y'all, thank you so much for being with us. This is clear tech loop. We're on the move and in the know. I'm Jo Peterson. I'm the CIO of clarify 360 and the chief analyst at Clear Tech Research. Y'all know me, but you may not know Mr. Todd Smith, who is the SVP and director of customer I am and threat intelligence at Ameris bank. Hi Todd.

T **Todd Smith** 00:28

Hey, good afternoon. Thanks for having me.

J **Jo Peterson** 00:31

Thank you for taking time to visit. If you're not following Todd, you probably should be, because he's a seasoned cybersecurity executive with more than 20 years of experience working at companies like Sofi, Barclays, Citi and the FBI, he currently manages seven direct reports and 20 indirect reports. So he's a little busy little bit, and he's got a global $2.7 million budget across the US and EMEA. So again, back to the little busy if you're new to cleartech loop. The podcast is a hot tech approach, and we're focused on cyber security, cloud security and AI security. And we each we each week, I should say we each We ask our guests three questions, and they're of the moment, right? So we all know AI, security is changing as quick as we can think about it. This is just a take of the moment. So let me get going with that. Let me ask the first question. Todd, give give me your thinking around shadow. Ai, is it an IT problem? A security problem, both, neither?

T Todd Smith 01:41

Well, I'll give you probably the easy answer, and just say both, you know, kind of puts it in everybody's wheelhouse, but at the end of the day, you know, it's something that everybody needs to be aware of when you're bringing AI into your environments, and why it's a both. Problem is security is going to own the risk there. You've got data leakage, you got IP loss, regulatory breaches. However, within those environments, it is the one that owns those controls. They're the ones with network available, network visibility, browser blocking capabilities. They're running, the API management, the firewalls. You can't isolate and silo the this issue, because if you do, that's where everything breaks down. You've got to have that constant communication across these teams. Granted, you should have constant communication across these teams anyway, but when you're specifically looking at AI, you're going to miss the mark if you kind of are putting it in one block or the other, because then, you know, you become a department of no as a security professional, because you're going to say, no, no, we can't do that. No, no, we can't do that. No, no, we can't do that. So if you bring in the IT group, they can say, well, you know, we can, we can formulate this answer. We can, you know, craft this posture. We can do this, that and the other, to make sure that this is a good solution, that is secure, safe, and get the job done for the company. There's been a bit of a vibe shift when it comes to that, I've seen, especially within my own company, you know, it's kind of figuring out who owned that. I think that's kind of the model we've introduced, is where security owns the risk and it owns the infrastructure and how to make it work. So, you know, it's something that is really speaking to a lot of like you mentioned today. It's from a strategy standpoint, something that needs to happen because it's going to enable businesses to move forward. And if you're the one that doesn't do the AI, you're probably going to be left behind from the others who are doing it. So specifically security folks, CISOs, CSOs, they need to think about enabling AI and working with it and not blocking it, because you're not going to be able to block it forever. Eventually, something's going to happen, and it's going to come through, whether you want it to or not. Got adversaries using it, your employees are going to start using it on their own, which is the worst example of any of any of them. You definitely don't want that going on because you're losing sight of your own data at that point, because it's going into an unapproved AI, maybe outside of your environment, they're copy pasting whatever it is screenshots. It's just a risk, so you need to basically enable them to use it in a safe and secure environment. That way it can also push the benefit, which then moves business forward and from every business I've ever worked for, mostly in the banking sector, that's what we want to see, is that move forward, if you don't, if you try to fight against it, say you're going to lose employees, you're going to lose customers, you're going to lose business, and then you're going to be looking for a job.

J Jo Peterson 04:37

That's fair. And I mean, look, you have peers in the industry, and we all talk to each other. I'm interested to hear what you're hearing from your peers about addressing shadow AI in their environments. How are they dealing with it?

T Todd Smith 04:51

You know, that's that's an interesting take, because especially in financial services and banking, we all have. Such different environments. Yes, we're all kind of the same thing. We're all banking industries, but our are all so different. Our different our core banking systems are different. You're either using third party or proprietary. It's all over the place. So how do you do it? How's the best way to structure it? It first, as with anything in this world, is knowing what you got, know your environment, know how to do it, know where you're going to be. You know, placing AI at the beginning, because you can't manage what you can't manage. So simply, gotta think of it as like a light switch. You're going to not going to flip the light switch on full blast. You're going to have a dimmer switch slowly, see how it works, scaling it up as it goes, and making sure you know that you don't shine a light too bright. And then everyone's kind of blinded. That also goes to the enablement, because then you can kind of walk into the walk into the relationship, walk into the implementation, and know where it works, and kind of keep your eye on what's going on. You know, Shadow IOI at the end of the day isn't going to be necessarily malicious. There's a lot of ended like I said, kind of going back to like, if you block chat, GPT, well, did you block Claude, right? Gemini, did you write every single one of them? You know? And you know, they pop up constantly. You know, a lot of companies now are at least having some semblance of copilot within them, but you got to remember which tab you're in, because there's a work tab and a web tab where you're putting the data into each that's something you mostly need to keep keep track of there, too. But again, it kind of goes back to the implementing, working through everything, working with everybody, working with the technology. Because at the end of the day, if you block it, they'll find a way. It's kind of like Dr Malcolm says in Jurassic Park, nature finds a way. Employees find a way.

J Jo Peterson 06:57

And you know what you're saying? So important, because I remember when email security was starting to be a thing, right? And forward thinking security folks said, You know what? We need, employee training on this, right? We need and so I see that there's an opportunity in the market for AI security training, right? I see that that's going to be an important because people don't know. Sometimes they just they they're not trying to do something wrong. They just don't realize they're doing something wrong, just like in on a bad email, right? It just we didn't know back in the day. You know that and right? So I think that what you said was really important about, it's just as much about, I don't see security anymore as the Department of No, I see it sometimes as the Department of Education.

T Todd Smith 07:55

Yes, I think that's a phenomenal way to put it. You know, especially in banking, financial services, everything's highly regulated, so there's a lot of web based training. You have to it annually. So, you know, stagger that approach make Don't bombard people with 35 web based trainings in the first two weeks of January. They're just going to click through it and nothing's going to unless you want to be really mean about it, and track the page, how time, how much time you're on each page, you know, I think I've been a part of companies that did that at my government, you know, and but there's some ways you got to do that, because you got to make sure that they get the training. Because I didn't know, is not an answer. So, you know, I think the Department of Education is a great way of putting it, because at the end of the day, you have to educate people about security. We have to educate our employees, our frontline staff, our bankers. And at the end of the day, we've really, really got to educate our customers, because any security procedure or policy that we put into place, the weakest part of that is going to be the human aspect of it. Obviously, as systems, we can secure those pretty well and at the end of the day, but the human aspect is where it is and, well, yes, I've already said, you know, I didn't know. Is not an excuse, but sometimes it's the actual truth. Not everybody's No, not everybody's gonna we think about security every all day, every day, right? But not everybody in any company thinks about security all day, every day. You know, you've got customer service reps. They want to help the customer, because that's what they do, and they do it well, especially at my bank, phenomenal customer service. They want to help the customer every day. That can be leveraged. You've got bankers who you know, they can help you whatever you need to do whenever you have financial hardships. They can help you through the toughest times of your life, they're not thinking about security, no about customer service, and that's their priority, and that and that that has to be true for for us to flourish. So we've got to be able to back them up as a security department and help them understand and help them be able to pass that message on.

J Jo Peterson 09:55

Yeah, that's a good way to because in their kindness, they could get exploited. Yes, right? I can see that, yeah, we

T Todd Smith 10:02

fishing tests not to catch you off. Jo, I've seen fishing tests where they come back and say, well, that's that's too harsh of a fishing test. That's fine, but the bad guys are going to be probably harsher. So it's okay, yeah, and it's just a test. It's okay, right?

J Jo Peterson 10:19

It's just a test to figure out where we are, right? So that's that's an important point of the two, because if you don't test, you're not going to know exactly I was super excited to talk to you, especially with the second question, because, given your role, I think this is something that every security person that I'm talking to is grappling with, NHS, right? Holy cow, that's

T Todd Smith 10:47

that's a nice way of putting it.

J Jo Peterson 10:49

I mean, right? Yeah,

T Todd Smith 10:52

it's one of those things that, you know, it goes back to the beginning of just really computers. At the end of the day, I've seen some really crazy start dates on NHS. It's, it's just, it's wild, because I think I've seen some estimates, you know, for every human employee, there's 10 NHIS go up to maybe 50, even 60, because you think I'm on you on board, you work. You leave, right, where's the cleaning crew to go in there and go through and clean every single NHI that you've ever made, ever made in your one year, or your 25 years of being an employee. It's, it's crazy. And this kind of goes back to the first question is, you know, AI in general, that could be a good way to help, help leverage this, send those, send that in there, and try to clean everything up. It's one of those things that are we too far down the road with NHI is to really have a clean house. Some of these companies might be if you've got hundreds of 1000s of employees, and then your times in that by 50 like it's going to be a task. But you know, at the at the end of the day, it's, it's a reality, and the discovery is what you really need to focus on. I've kind of been a been a thread through this whole conversation so far. Jo is, you've got to know what you have. You've got to know, right? And at the end of the day, one of my biggest things, and I kind of cut my teeth in my beginning of my career as an intelligence professional, I don't know what I don't know. So all you can really do is the best you can with those NHIS identify as many as you can figure out a way that's good for your company and good for your risk tolerance. Go find them. You know, do some hunts, go get them. They're out there. And then, you know how you want to triage those moving forward, you've got to stop the bleeding and then prevent the bleeding, because if you're just, if you're catching everything on the back end, that's old, okay, but now you're adding to it every, every day, every month, when people leave, you're kind of, you're you're cleaning it up, but it's still getting messy, so you've got to really figure out how to thread the needle of clean up the historical clean up the present.

J Jo Peterson 13:08

Yeah, interesting, I mean, interesting problem and not easily solved. Last question that I have for you, when you hear the term AI defense, what comes to mind for you?

T Todd Smith 13:23

Oh, there's so many ways you can look at this, however, kind of perspective you want. It's such a big question, which you know is great for a podcast. You know, how do you look at it is, is AI your defense? You know, is AI coming at you. And so, you know, like, how do you look at a AI defense? Are you defending with or are you defending the AI day? You know? So for me, specifically, when I look at AI defense, because probably at the stage we are, and what I've seen more recently is it's going to be the AI within. So I've always kind of used the the term, you know, we don't want it to Sky net, you know, to date myself as a terminator fan, you know, we don't want to inject AI into one area. And the guardrails are a little lax. The security protocols on it are lacks and it's spreading, yeah, you know, so we don't want it to Skynet. So that's really AI defense. That's how I think of it. First again, it goes back. You got to know what you have. You got to keep your own house in order first. Because if I've got aI inside, what is that leveraging? What is it looking at? How is is it exfiltrating? Anything? Right? Oh, what's going on in your house? So really, you're kind of defending against your own AI to start, that's where you need to build your foundation, leverage it inside. Know what's going on, how it's working, what it's doing, where it's looking. One of. Of things too for that, NHIS. What is it doing with NHIS? Are they communicating what's going on there? How are people accessing and leveraging the AI? Are they allowed to access what they're allowed to access through AI? Or can they sneak over in another area and pull data? Really, it's defending the AI within, and then after that, you got to defend the AI from without which that is what we're talking about, the security part, the shield, if you will, and because AI threats coming at you are coming daily.

J Jo Peterson 15:31

Yeah, that's true. So so many good things. I hope you'll come back and visit with us again, because this is an evolving conversation. Obviously we're all just sort of learning how to deal with stuff, and the playbook for traditional security is a little bit different than this, right? Just is. So, yeah, 100% so thank you so much for your time and looking forward to chatting with you again.

T Todd Smith 15:56

Thank you, Jo, appreciate having me.