CTL-CISO-Patricia-Titus

Tue, May 26, 2026 5:51AM 16:26

SUMMARY KEYWORDS

AI security, shadow AI, CISOs, visibility, governance, risk management, data governance, AI agents, non-human identities, zero trust, cyber hygiene, API security, thought leadership, innovation, executive awareness.

SPEAKERS

Patricia Titus, Jo Peterson

J **Jo Peterson** 00:07

Hey everyone, thank you so much for joining. We're here today with Clear Tech Loop. We're on the move and in the know. I'm Jo Peterson. I am the CIO of Clarify 360 and the chief analyst at ClearTech research, and I'm here today with Patricia Titus. Hi, Patricia.

P **Patricia Titus** 00:24

Hi, Joe. How are you today?

J **Jo Peterson** 00:27

I'm good, thank you. So much for making time.Patricia TitusIn case you guys are not following Patricia yet, you should. She's a seasoned CISO with 25 plus years of experience leading security organizations across both public and private sectors, including financial services, technology, and government, Patricia has designed, implemented, and transformed global information security programs, earning recognition as a trusted leader in this highly regulated industry. She's held C-level and executive positions at Booking Holdings, Markel Corporation, Freddie Mac, Symantec, Unisys, and the TSA, and one of the things I admire about Patricia is that she is passionate about advancing women in cybersecurity. Patricia actively mentors future leaders and serves on the executive board of the Girl Scouts of the Commonwealth of Virginia, and the Board of Advisors for the Executive Women's Forum. So, thank you for all your efforts in that space, Patricia.

P Patricia Titus 01:32

You're so welcome.

J Jo Peterson 01:34

And, I, you know, in case you guys don't know, the Girl Scouts are way out ahead of things in cybersecurity, they give little badges to the Girl Scouts that complete cybersecurity training, which is just like the cutest thing. So, but today we're here to talk about AI security, and if you had a chance to listen to the podcast before, you know that we're a hot take approach. I asked three questions in short order. Patricia gives us her thoughts, and we're just of the moment, because, as you all know, AI security happening is happening in real time as we're looking at it, right? So, first question I'm going to ask you, Patty, is: Give me your thinking around shadow AI. Is it an IT problem? Is it a security problem? Is it both? Is it neither, and how are CISOs addressing shadow AI in their environments?

P Patricia Titus 02:25

So, it's both, so it's both a security and an IT problem. And, as per usual, CISOs have to figure out how to work collectively with the CIO team, because more specifically, I'd say it's a governance plus a risk plus a productivity problem that shows up as an IT issue, and it's an IT issue and fails as a security issue if you don't get ahead of it.

J Jo Peterson 02:57

Yeah, super fair. And how are they addressing it? How are you seeing them address it in their environments,

P Patricia Titus 03:03

So they need to get serious visibility. So, what I'm seeing my peers doing is trying to come out with the safe path and enforceable guardrails, but it all starts with visibility, because if we don't know what's going on and if we're not asked to participate as a trusted entity, it's hard for us to set that safe path and those guardrails, so we have to create approval lanes, which are genuinely easier than going rogue, and that's a tall order for a CSO, right, so most frameworks put specific stopping points within the process, so that we can risk and we can do assessments, and we can scan apps, or you know, whatever it is we're looking for to really mitigate the risk for the company. This has to be different. This really has to be approval lanes that are simpler than people saying, well, I'm just going to not tell security, and we'll just figure it out later. We really have to enforce the AI risk management by design, if I can coin the phrase, like security by design or privacy by design, we've got to anchor controls in with the data governance component, because it's really about consumption of data in order to make those AI models work, and if we treat AI agents, because I think that's kind of where we're at right now, it's really the agent piece. The LLMs, I feel like people are being a little more purposeful about those, like the agents have, like, gotten loose, like gnomes in our systems, and they are just. Just out there, gremlins, maybe would be a better term, and it really, they're new, they're a new control plane for us, and so we got to build some governance around the agents, because those are already, you know, like bot agents, AI bots have been around for

J Jo Peterson 05:17

right

P Patricia Titus 05:17

time now, they're just getting better, and now they're getting to the point where they're talking to each other, and maybe able to cut the human out of the conversation, and that's where we have to get smart about it. So, it's really a cross-functional governance, and we got to stop pretending policy alone is going to control it.

J Jo Peterson 05:38

So, yeah, right, and I was talking to Rock Lambros last week, I don't know if you know Rock, but he's really focused in AI security, and we were talking about Mult Book, so it's, it's just crazy, it's crazy, any thoughts, Multiple,

P Patricia Titus 06:00

about, I'm sorry,

J Jo Peterson 06:01

mold book, you know, that claw bot, that agent platform.

P Patricia Titus 06:06

Oh yeah, that's not.. yeah, that's a pretty frightening.. you know, I gotta tell you, I'm that kind of thing comes to light, and I'm thinking, oh, there it is, what we all thought, we all didn't want to say out loud, because we were afraid if we said it, it would happen to us, and it happened anyway. So it's, it's, it's kind of like, yeah, I think we didn't want to project it onto ourselves, but it's happening, and I'm happy that happy is maybe not a good term, but I'm glad that it's happening now, where we can somewhat try to contain it, because some organizations have not embraced it yet, and so it helps us say not say we told you so, because we haven't had enough time to actually say I told you so, to actually try to come up with layers for how we secure what are we going to do to put things in the appropriate sandboxes where we can enforce some of the controls, so I think we have to continue to invest in education, and that's where things like Clawbot, I know a lot of companies that are early stage are trying to hurry, and part of the hurrying is using, you know, technology to try to enable faster moving. I always get nervous, though, when I hear CISO saying, "Oh, I'm doing some Python coding, or "I'm vibing, or "I'm just like, are you doing it? And I'm like, "Not now, I have people. I'm fearful if I did it. It's kind of like, yeah, but a lot of people are using, you know, what you can do with, with, with club, you can actually like write code, and I'm like, that's great, I don't, I don't need to do that right now, because I'm not a coder, it's, it would be like, it would be like saying you can use AI to build an airplane engine, I'm not doing it. I'm not going to put myself in the airplane after I built it with AI, because, like, you know, there's a trust but verify component that I don't know how you verify it, unless,

J Jo Peterson 08:33

right, unless you're like you're in the plane and you're hoping you're praying it's gonna fly, right? No, that's right.

P Patricia Titus 08:39

I mean, you got to have that's when you got to pack your own parachute, if I can coin it.

J Jo Peterson 08:46

So fun, but I'm so glad that you brought up the education part, and I hadn't thought about it the way you were seeing it, where it is kind of a good thing in a way, because you know what, it's evidence, right? So we raise up our hands, and we say, "Oh, there's a problem, and you know, board, you need to get serious about it, and, board, we need to tell you about it, and they're like, they can't get their minds around it, because you don't have anything to show them, here's something to show them, here the bots are, if I'm getting it right, and I've seen a little bit about it. The bots are actually talking about how humans are listening to them, and they're taking, and we're taking pictures of them and posting them on social media, right? So it gives you a dialog to open with an executive to say, I need to shut this down. How do we go about doing that, right?

P Patricia Titus 09:39

If we do, if we think of 2001 Space Odyssey,

J Jo Peterson 09:45

yeah,

P Patricia Titus 09:45

that's like predicted, but to be honest with you, we have this now new awareness, and if we have detection without awareness. This, the detection just becomes theater. In other words, if we're out there talking about it and saying, "Oh, this thing could happen, it's like 2001 Space Odyssey. Yeah, but 2001 happened, and we were all still alive, and, yk happened, we're still here, you know, all these things where there were some security theater around it, it creates an unintended consequence of the Peter Cried Wolf problem. Now we have fact that we can ground people in.

J Jo Peterson 10:33

Yeah, no, that's a really good way to sort of think through it. So I would love to hear how you're hearing about CISOs and CIOs actually enabling NHIS and how they're accounting for them, because I'm hearing all kinds of different stories. I don't know about you.

P Patricia Titus 10:54

So, interestingly, I did a podcast not very long ago, and one of the participants was talking about the fact that we created this problem today that we didn't think would be a problem yesterday, where we separated human and non-human accounts and identities, and so by doing that bifurcation we couldn't have predicted today, you know, 10 years ago,

J Jo Peterson 11:26

right?

P Patricia Titus 11:27

And that bifurcation now has gone like this, where we're now so connected with the human and the non-human identities that it's so challenging to tell the difference between the two. Now, the good thing is, with a human, we have a human form, and we call it cradle to grave, which is a horrible way to say it. A person's life and a company is the birthright, and then the termination, which sounds.. we know when a person starts and when a person terminates,

J Jo Peterson 12:00

right?

P Patricia Titus 12:00

A problem with the non-human accounts and identities is we haven't done such a great job of that birthright, let alone what we're allowing it access to. And when we decide to terminate it, let's go back to that clog bot conversation.

J Jo Peterson 12:22

Yeah,

P Patricia Titus 12:23

what if the clock? What if the bot? What if the AI agent says, because our fail-safe is shut it off. I mean, you just

Jo Peterson 12:30

exactly.

Patricia Titus 12:31

Yeah, what if he says no, you're not.

Jo Peterson 12:33

Yep,

Patricia Titus 12:34

and it starts internalizing human emotion of survival, and it figures out how to stay on, and the bigger problem that we have with non-human identities is proving to an auditor, I shut that agent off, that that non-human identity has been turned. How do you prove that, and how do you create like this is really how to create enforcing least privileged by default. Some, you know, some people talk about zero trust. Zero trust, I think, in my mind, is a pipe dream. I think some organizations are defining it differently, therefore being able to call it done. Done. Let's toss agents into the mix. So, does that throw a wrench in your zero trust?

Jo Peterson 13:30

Yeah,

Patricia Titus 13:31

but if I remember, and maybe you'll appreciate this, because you're more on the CIO side, more on the technology side. When we started trying to do like service account cleanup, non-human identity service accounts, and then all of a sudden we founded nested and nested and did, and you know, nth layer of service accounts that we didn't even know what they went to, because we had terrible naming conventions, and

Jo Peterson 14:01

right,

P Patricia Titus 14:02

and I had one CIO that, bless his heart, said just turn them off, and we'll see who screams, and I'm like, yikes, is there a good time of the year to do that, like maybe not at the end of the year during financial close, or maybe not, I mean, there's never a good time to turn something free baseline, and then non human identities that we don't talk about are APIs.

J Jo Peterson 14:27

Absolutely,

P Patricia Titus 14:28

we don't talk about APIs being part of this. We just let APIs be everywhere,

J Jo Peterson 14:34

everywhere,

P Patricia Titus 14:35

and it's another potential threat surface or attack surface that we're going to have to account for at some point.

J Jo Peterson 14:44

You're right, and it brings to my mind a big, a bigger, you know, it seems to me that only larger organizations with bigger benches and or very technically focused organizations even focus. Focus on application security, right? So I say to them, like, what are you doing around, you know, APIs? How you.. how you.. and I get this kind of blank stare.

P Patricia Titus 15:11

Yeah, yeah,

Jo Peterson 15:12

you.. I mean, because they have it, they just don't have the bandwidth. Sometimes they don't have the bench. I'm not picking on anybody here.. budget bench, whatever it is to really get their arms around that,

Patricia Titus 15:24

yeah.

Jo Peterson 15:24

So,

Patricia Titus 15:25

so what? When, when I think about AI defense, I think it's less about the novelty of it and more about reapplying fundamentals at a new scale and velocity. We haven't done a great job with the first one of of the defenses and the cyber hygiene pieces, and now we're adding another layer of complexity. So, I think this is a great time for thought leadership and innovation in this space, and I think that's actually happening.

Jo Peterson 15:57

Yeah, that's very fair. Well, thank you for your insight. It's so good, and such a pleasure to have you on the podcast. And I'd love to have you back if your time permits. So, I guess maybe we'll see you next time.

Patricia Titus 16:12

You bet. Thanks, Jo

Jo Peterson 16:14

Thanks.

P Patricia Titus 16:14

Bye.