CTL-CISO-Fernando-Montenegro-v2

Fri, Feb 27, 2026 6:33AM 20:11

SUMMARY KEYWORDS

Cybersecurity, generative AI, cloud security, AI adoption, security controls, innovation, empathy, threat modeling, organizational governance, strategic trends, CISO role, technology vendors, risk management, collaboration, strategic decisions.

SPEAKERS

Fernando Montenegro, Jo Peterson

J **Jo Peterson** 00:07

Hey everyone, thank you so much for joining clear tech loop. I'm Jo Peterson. I'm the vice president of cloud and security for clarify 360 and I'm the chief analyst at Clear Tech Research. And I'm here today with Fernando Montenegro, hi, Fernando.

F **Fernando Montenegro** 00:22

Hello, ma'am. How are you today?

J **Jo Peterson** 00:24

I'm doing great. Thank you for making time to visit.

F **Fernando Montenegro** 00:27

Of course.

J Jo Peterson 00:28

Y'all. If you are not following Fernando, you need to. He is the Vice President and Practice Lead for cyber security for the future group. He is one of the sharpest security analyst I know, see shaking his head, but it's true. And I think what makes him such a great analyst, in my humble is that he was an he's an engineer by trade, and so he really understands the tech and how it fits together in the landscape, the customer's landscape. He's not going to say anything nice about himself, so I'm just going to have to say wonderful things about him. Guys, if you're new to the podcast, we're a hot take approach, and we focus on cybersecurity, cloud security and AI security, and we ask each guest each week three questions, and our goal is to educate our listeners here and now real time, so without further ado, first question Fernando, how can cybersecurity professionals leverage generative AI to break out of what's been a very traditional tools and tech mindset and drive more innovative thinking and execution in their security programs.

F Fernando Montenegro 01:45

They have to jump into the pool with it, right? So this is a hot take. They have to jump into the pool

J Jo Peterson 01:51

all right.

F Fernando Montenegro 01:52

What I mean by that is that AI generative AI, so by the way, by I've been around the block for a while. And the joke I like to say is, like, like Elrond in Lord of the Rings talking to Gandalf. I was there Gandalf. I was there 3000 years ago. I've been around AI, not since the 1950s No, but like, I've lived through one, I've lived through the second AI winter, right? That happened in the in the 80s and 90s, right? And so I've been around the block for a while, and the thing I can tell you is that I, the thing I find fascinating about AI, like it warms my heart, is that it is one of the most interesting technologies that I've come across in the context of bringing together technology and business, right? And like, I love cloud, I've covered cloud for years. That's how we first met. The cloud. For all the phenomenal things about cloud, and trust me, there are, it's still very technical. Ai. On the other hand, bridges the gap between technology and the business in a way that I haven't seen anything else do so far. So my recommendation to practitioners is you have to jump into the water to understand what's going on and and the way that you break out is, okay, you use AI. First of all, you don't deploy it day one on your mission critical production system. But the way that you do it is you experience, okay, what is this gen AI, thing, I strongly recommend people take a look at what is the actual technology, right? You don't need to read the Transformers paper like the attention is all you need. Paper from 2017 that's not it, but you need to understand, okay, it's based on novel neural network architectures. Great. What are neural networks? Oh, neural networks work this way, and then have layers and have back propagation and on and on and on, right? Because once you understand what the technology is. You have a better grasp of what you can and what, most importantly, what you can't do, right? So I say jump in both in terms of understanding what the technology is and it's not, and using it on your regular cases. I use AI on a regular basis as a sparring partner. I use AI as a glorified search engine, right? I use AI to help me with the with coding, right? I write horrible, horrible plural looking Python code, right? But I I was able to use by coding whatever you want to call it for languages that I'm not as proficient as, like TypeScript or something like that. So anyway, sorry, I'm belaboring the point. I think that the way that you break out of the tool and tech mentality is you learn where it actually works in your use cases. And you are going to find quite a few places where. It's great. You'll find a few places where it's not and that's, that's where you bring your judgment of the professional to a look. Let's apply it here. Let's apply it over there.

F Fernando Montenegro 05:11

That's a good answer. And you bring up such a valid point, because I'm starting to see folks have conversations that, and I mean specifically CIOs and systems. Now, a lot of them already do talk, and a lot of them are friendly, but some of them aren't so friendly, right? If we're honest about it, and I'm seeing these conversations occur where they have to work together, where the silos have to come down in order to get AI to work, right, just and you're right. That didn't have to happen in cloud. The infrastructure guys in cloud could go do what they wanted to do, right? Nobody was the wiser. So, yeah,

F Fernando Montenegro 05:58

so, but yeah, so once we jump into it, right? Once you start using it more, you are in a better position to see the potential. Because I think that to pick up, I love the way you framed it, like that, we have to bring these silos down. And one of the ways to bring these silos down is to have empathy for the other side, if you will, right? And if, if security teams can can see the potential within their own world of what generative AI can and can do, they can get a glimpse of, hey, perhaps that the business users and the it, they are so excited about this, because I saw what you can do for me, I can only imagine what you can do for them, right? So it brings people together, right? So I think that the way you break out of things is to use it so you understand it better, so you can work with others around it better.

J Jo Peterson 07:01

Yeah, really. Good point, and in that same vein, because for years, security has been known as the Department of no right. That was the running joke, of course. So how can organizations still embed security and privacy controls into AI model development without slowing down innovation.

F Fernando Montenegro 07:23

So this is an important one in the context that I wish I could give you a ties open up. There's a perfect answer to this problem, and this is just like, No, there isn't right. I think that the way that you embed privacy security into this into this initiative is by being there early and by helping them, by helping that initiative flourish again. You understand what they want to do, and you are yourself equipped enough to bring in. Look, this is where things break. This is where it's different. This is, these are the the issues that we are likely to have. So help let me. Let me. Help you. Help me. Help you. As a, as a, as a as, as the security practitioner in this AI initiative that we have, right? Let's, let me pinpoint for you, what are the key areas of where we are concerned about something. And let me help you by creating. I love the paved path approach, right? I allow me the, let me do the heavy listing of analyzing some of the models that you're doing that you want to use, analyzing what the use cases are of working with your team on a very lightweight threat model exercise, right? And then if we can get rid of, if we can, if we can tackle the conceptual security issues around AI usage early on, right? It becomes, it becomes that much easier to it's just a little bit of friction early on to figure out where you where you want to go. That makes the whole journey that much easier. I love bad analogies. It's a bad analogy of, let's say that you want to go so I live just outside Toronto, right? And let's say that that I want to go to New York City, right? It's the difference between me picking up before I start on a journey, looking at the map, and figuring out, oh, okay, I have to go down this particular route. I can cross here. I can go there, there, there. It's those few minutes of Oh, yeah, by the way, oh, look, I probably. Going to need to fuel around here, here, here. It's that initial planning and initial consideration a little bit on, rather than just getting into my car and driving right so, and we all do this instinctively, right everywhere. We always plan for things. I think that we're, frankly, where I think that sometimes we run into problems with with security and AI is because, to your point, we are the department we were known as the Department of no 100% if that's the if that's the vibe, pun intended, that we're bringing to the conversation, then people are not going to want to talk to us, because nobody wants to, right? And then we're going to come back at the end as the as the party spoilers, right? Or because, hey, oh no, no, you can't use this as insecure. If, if we had been involved from the beginning, things would have been so much different, right? So I think that the way that we embed it into the into the the effort is by being there at the beginning, by having empathy for what people are trying to do, for having the right level of knowledge about what they are trying to do with AI and I go back to, okay, this is why these models work this way. Why these models work that way? You want to use the this third party to do this? Oh, let me tell you, by the way, this kind of data sharing with the third party, it's not something that our our company, may be comfortable doing and but you solve all of this at the design stage, at the initiation stage, not down the line when people want to release the production. Sorry, long winded answer, but it's a you got to be there. Like I wasn't it. Was it the Woody Allen or the Beatles who said that like 90% of life is showing up or something like that?

J Jo Peterson 12:01

I don't know, but Okay, so you referenced Gandalf, you referenced Jerry Maguire, right? And now I'm going to ask you to reference and put on your your Wizard of Oz CISO hat, Wizard of Oz CISO hat, and be thinking about AI adoption, and and tell me how to balance for an organization securing emergency, emerging threats. And then the other side of that coin, organizational governance. Where do you come in?

F Fernando Montenegro 12:39

In terms so I like, as analysts, we cover many trends happening, and I'm not going to go into all of them. One of the major strategic trends that we're seeing that that like I've been in this industry. I've been around this industry for 30 years, yeah, one of the industry, one of the changes that we're seeing is there is this undeniable strategic list to cyber security, right? It is now. It has been for, I don't know, 510, years now. It has been board level conversation, right? It has been career making or breaking, for, for, for people, right? I like to think that I say that so Mark and Peterson had that famous quote in the early 2000s or late 2000 late 2000s early 2010 Software is eating the world, right? He was right, right. It did eat the world. Everything we do around technology. So as technology becomes more important, more strategic, it changes how we make decisions about cyber security. What influences the decisions about cyber security, right? And it's the kind of conversation where, well, now perhaps making a choice between Model A and Model B also has to factor in geopolitical risk of where that provider is located. Well, we weren't thinking about geopolitical risk. Of some of us were, but like as an avid net, a smaller set of the user population was thinking about geopolitical risk years ago, right? Or the fact that this particular technology decision we're going to make is influenced by our our insurance coverage, or this particular alignment has to be done in light of this particular set of regulations or regulations, whether it's industry regulations or or national or state loss right anyway, where I'm going with this is that this is changing the nature of what it means to be a security professional. Whether you are a an engineer who is working on things, whether you are a first level, mid level management who's working on things, whether you are a senior manager working on things. So that particular CISO hat that that you were bringing up, it's not just one hat, right? It's nine or 10 different hats, and some of those different hats are to be used in relation to the CIO, in relation to the board, in relation to the development teams, in relation to the rest of the company, in relation to the customers, in relation to General Counsel. So we're asking, I promise you, there's a point to my madness. We're asking that security executive for them to be that much more worldly, right? So I mentioned this because to go back to your question, the balance between emerging threats and governance and trust, right? If that, that CISO, that security executive, they are playing on all sides, they are playing multiple games at the same time, and they have multiple roles at the same time.

J Jo Peterson 16:14

Yeah,

F Fernando Montenegro 16:14

right. One of the most important roles that they have is as the translator of things right? They are the translator of security issues to non security decision makers. They are the translator of business constraints to security teams. They are the translators of of security requirements that are coming in from outside regulators, from from your from your customers, from your business partners. I mean, how often do we now get to see CISOs either directly involved or somewhat involved in justifying the company's own security posture during a failed process? Absolutely no. What I mean by this is that it's not about coming down to one side. Oh, let's focus on emerging threats, or let's focus on governance and trust it. How do we play all the sides all the time? Right? To use another bad movie, reference, everything, everywhere, all at once.

J Jo Peterson 17:19

Right? Here. Right? You get a million of them. I bet you get a million of them, but you make such a good point. I remember studying for the CISSP, and I thought, oh, it's going to be all technical questions. And exactly, I was just so surprised at all the risk questions, and now they were so wise having all those risk questions in there, because that's such a big part of the job.

F Fernando Montenegro 17:49

And the part of the job now is changing as well. The job is, it's not a dirty word, but the job is more political. Now,

J Jo Peterson 17:58

absolutely, the job is more collaborative. Now, the job is more consultative now, and part of the reason for that is because,

F Fernando Montenegro 18:08

again, technology security has become that much more strategic, and as it became more strategic, another consequence is that you now have technology vendors that were not traditionally security vendors.

J Jo Peterson 18:23

Oh, yeah,

F Fernando Montenegro 18:24

significant amount of security functionality into their products. Well, the decisions about those product acquisitions are not security, right? You're not going to ask security to choose your to choose the entirety of your estate. Who's going to choose your your what workstations your people use, or what database is going to be used? But security has to be involved in those conversations, right? So it changes the nature of what we're doing to be that much more collaborative, to be that much more involved with the stakeholders who are actually making those decisions with the input from security. Right in some organizations, that input from security is going to be a strong suggestion. In some organizations that input from security is going to be a it's going to be a showstopper, a showstopper issue. If security needs are not met, it varies and the CISO they need to be able to navigate, which kind of organization are they on, which kind of problem they are solving. Sorry, I again, I went on a rant, but it's a, it's a, it's a fascinating topic to be a fascinating time to be in this industry,

J Jo Peterson 19:43

it is, and with that, it's a fascinating opportunity for me to get to collaborate with you and share some thoughts. So it's been lovely. Thank you so much for giving your time today, and everyone, thank you for joining and we will catch you next time. Absolutely. You.