CTL-CISO-Gerry-Gadoury

Sun, Mar 08, 2026 11:43AM 11:29

SUMMARY KEYWORDS

AI security, generative AI, cybersecurity, social engineering, risk assessments, innovation, privacy controls, CISO, organizational governance, business aspect, technical solutions, executive alignment, ransomware, shadow AI, risk management.

SPEAKERS

Gerry Gadoury, Jo Peterson

J **Jo Peterson** 00:07

Morning clear tech loop. As you know, we're a podcast on AI security and cloud security, and I'm here today with Jerry gudori, the CEO and founder of red beard solutions. Hi, Jerry.

G **Gerry Gadoury** 00:23

Great. Thanks for having me on Jo,

00:33

o

J **Jo Peterson** 00:34

disabled veteran owned professional services firm that has a strong focus on cyber security and tech, and they work in the federal and private sectors,

G **Gerry Gadoury** 00:45

correct? So

J Jo Peterson 00:48

again, appreciate your time, Jerry, and let's just get started with the questions. Awesome. As you know, everybody that joins the podcast, we asked three questions, and today's no exception. So the first is, how can cybersecurity professionals leverage generative AI to kind of break out of that traditional tools and tech mindset and drive more innovative thinking and execution in their security programs? Sure. So my first introductions to cybersecurity was back when phone freaking was a thing. So I say all

G Gerry Gadoury 01:26

the company's name is red beard solutions. But if there were truth in advertising, it would be gray beard solutions. So I mentioned that to say that generative AI is the latest kid on the block in the Tete, a Tete between the bad guys and the good guys. So the number one thing that I would recommend is to make sure you're staying abreast of the changes. Don't forget the human component. Social Engineering has always been the easy way in and make sure that you're again, you're seeing what your peers are doing, but also what the bad actors are doing.

J Jo Peterson 02:01

That's a great answer. You got to stay current, right?

G Gerry Gadoury 02:04

Yes

J Jo Peterson 02:04

this stuff doesn't slow down. The next question is, how can organizations embed security and privacy controls into their AI model development without sort of slowing down innovation?

G Gerry Gadoury 02:20

Yeah, you know, again, I have such a strong tendency to go back to the to the social component, and in this differ slightly and say that do real risk assessments. I think that sometimes we focus too heavily on what could happen in we we don't, we don't cover what, is likely to happen, and sometimes that over compensation creates a weight that slows things down too much and impacts user adoption. So that would be my advice. Do real risk assessments. Don't look so much for the Boogeyman. Look for the person actually knocking on your door.

J Jo Peterson 02:58

You know, it's so interesting that you said that because I was at a conference last week and they were talking about non technical executive table tops around ransomware. And what was funny about it was that, and it wasn't funny, but when the one of the CISOs was telling a story about how they suck, all the executives in the room, everybody, you know, CFO CEO, all the stakeholders and everybody was fighting about the fact that their thing, whatever they covered, was the Most important thing to the company, right? You're smiling.

G Gerry Gadoury 03:42

Nature, yes,

J Jo Peterson 03:43

right, normal. But they, you know, they couldn't get alignment on. Hey, if the you know what hit the you know where tomorrow, what do we do? What do we need to get the business, at a minimum, up and running, right? And they hadn't really had that con- All the technical folks had run books and playbooks and but they hadn't really sat down with the with the executives to talk about that. And the perspective that they got from that was really interesting about what everybody thought was important.

G Gerry Gadoury 04:17

You know, I make a big deal out of it when I'm talking to CISOs and other cybersecurity executives not to lose the human piece their interaction with their teams not only impacts their own success trajectory. I mean, gosh, we've all worked with companies that that believe security should be mandated, not sold, and the end result is always resistance. The inverse what you're describing and understanding the executives concerns, mitigating the necessary fears, and getting them on the right track is so important. I mean, obviously we're tech folks. We care about the technical solution, but we can't lose sight of the fact that the other word is solution. Yeah, that's a really good point. I like that.

J Jo Peterson 04:59

So. Let's take a minute and get your perspective on how the CISO, because I always think of it as a balancing act, so I'm really curious about how you think about it. If, on one hand, we've got al adoption in terms of its use to secure emerging threats, right? So what can it do for me in security, but from an organizational governance perspective, how should the CISO be thinking about these things and then trying to balance them?

G Gerry Gadoury 05:29

Yeah, that's a great question. I'm gonna and I hope this doesn't come up as a block so so feel free to hold my feet to the fire. I don't really answer your question. I'm reminded of the late 90s, early 2000s when the CIO/CTO was just earning their seat at the big table. And CISOs are in a very similar place now. And and and they need to accomplish the same things that CIOs and CTOs did then, which is to say they have to understand more aggressively the business aspect of the decisions they make. If you remember back to the 90s, a lot of CIOs were like little kids in a toy store. They were making changes because they were cool and it was the cutting edge stuff, and their inner nerd wanted to play with the new toy, and they were failing to understand the business ramifications. I say that because I'm guilty of it. So I feel okay making that shot or taking that shot, but they had to better understand and the.com crash kind of taught them, in a hard way, that their technological changes needed to be supported by the business there need to be a business reason why. I think CISOs now really need to ensure that the decisions they're making, again, going back to a risk assessment, are following probable avenues of attack and make sense for the organization involved. So I don't know if I'm answering your question well, but I would say they need to. They need to make sure that their adoption is rapid enough that their organizations are are protected, but not so rapid that they're beta testers.

J Jo Peterson 07:06

So what I'm hearing you say is the Department of maybe,

G Gerry Gadoury 07:11

yeah, I know. I hate saying that. It's such a dodgy answer, and I'm I just I don't know that there's a blanket answer can be different than about if I'm Jerry the the CISO of a manufacturing company that makes ball bearings, they're different things that will have, I think, very different answers,

J Jo Peterson 07:35

yeah, and I think you nailed it right there, right? If I'm in a super regulated industry, and on the CISO, I'm way more nervous about shadow AI and the stuff that's going on, right, and exfiltration and all that stuff. Then if I'm, you know, making ball bearing somewhere, right, or or planters, or whatever, so I get it right, and it's and you're going to think about it differently, if you are. It was interesting. I remember studying for the CISSP, and a lot of the questions were about risk. You know, I was thinking that they were going to be about security, right? But they were about risk. And I remember one of the lessons about studying for the test was that, you know, they're trying to train a risk officer. And and I think about that when I think about AI, because I feel like, and I'd love to get your perspective, that the CISO needs to be thinking about risk even more than before.

G Gerry Gadoury 08:46

Yes, the world has become less certain. AI is such. Do you remember back in the day when we used to tease non technical hackers and call them script kitties?

J Jo Peterson 08:59

Oh yeah,

G Gerry Gadoury 09:00

for sure, they're, they're technical masters compared to what you need to be now to enact a pretty sophisticated AI attack. So the platform of understanding that we're operating under is fundamentally different, and it's only changing more more quickly. I mean, gosh, again, AI is, is such a new kid on the block that the AI landscape changes fundamentally by quarter. That's probably the two so staying current with changes and differences. And I know CISOs have a love hate relationship with vendor sales people, and I get that but, but they can be your best friend, if you can have a strong enough relationship to have them not go full pitch mode every time they open their mouth and share what's really changing in their platform, products and services?

J Jo Peterson 09:54

Yeah, I was on a call this morning about vendor X. Rolling out an AI specific firewall.

G Gerry Gadoury 10:04

Wow,

J Jo Peterson 10:04

right? I mean, think about that a minute like, huh, come again. Say that again. So lot, lots of changes

G Gerry Gadoury 10:17

at last year's big cyber tech conference for government in Maryland. The two buzz words that everyone was talking about was zero trust in quantum computing. And I'm just wondering when quantum computing enters the field and combines with AI that quarterly change is going to be a darn near daily one. So,

J Jo Peterson 10:38

yeah, I don't even know what that's going to look like it's a lot to think about, isn't it?

G Gerry Gadoury 10:43

I'm reminded of the 1990s movie, sneakers, about algorithm. Do you remember that no more secrets? I'm reminded of that movie.

J Jo Peterson 10:54

It was great. No more secrets. Yeah, great. But no, this is fun conversation. Thank you again for taking time to visit with us. And have to have you come back and we'll talk MCP servers or something ephemeral, agents or something else scary. How about that?

G Gerry Gadoury 11:13

That sounds great.

J Jo Peterson 11:15

Thank you again.

G Gerry Gadoury 11:17

Welcome Jo.