THE RHODE ISLAND CEO COUNCIL

*An Exclusive Consortium of CEOs Building a Stronger Rhode Island*

June 9, 2022

# CEO Briefing

## *What CEOs Need to Know & Do About Cybersecurity*

Transcript of CEO Q&A with Panel of Cybersecurity Experts: Kiran Mantha, Todd Knapp, & Jason Kravitz, facilitated by Heather Wilkerson

**Question:**

What can we do, if anything at all, when it comes to trying to control employees shopping during the day? They go to Macy's (laughter). And I think – forget the time waste – just does that make me more vulnerable - because they may have gone into an unsecure website, they're going to Target, they're doing their pick-up groceries from Stop and Shop, or whatever it's called, is there a way to control that?

**Todd Knapp:**

So, my opinion is that when you talk about sites like the ones you're describing, that's really the lowest level of threat from a detection and management point of view right now. The technology is pretty good at that. We're not likely to find ourselves with even basic good technology around our networks getting compromised, because somebody went to Amazon.com. I would also argue that, culturally speaking, the world's shifted a lot. There was a time when everybody brought briefcases to work, right? And they were - they would sit at their desk and every once in a while, they open their briefcase, and maybe there was a newspaper in there or a brochure for their vacation or something like that. They worked on paper; they relaxed their brains on paper. Working in the digital world is very, very consuming of mental energy. I think people need those moments of being able to step away for a second and do something - And clearly there's a line where we don't want to - I mean I've got a team, too - I don't want to lose productivity on them also. But I also think that the biggest problem with the whole model is that the moment we turn IT into police officers with stuff like this, we lose the trust of the user base and the whole game's over. They're never going to report it when they've made a mistake for fear of being on the wrong side of that policy line. So, you know, I would say the trick is to harden the edge of the network and the technologies you've got for detection, and then, you know, keep an eye on it and deal with the real problem users, and skip the rest.

But on the whole, you feel like a lot of systems aren't really geared towards finding and sort of stopping that side - sort of malware.

Yeah. And I'm dealing with attacks every single day with clients - we have a cyber practice. I'm working on nine different events right now that are brought to me by various agencies. I don't have anybody that was attacked over something simple like that. They're getting smacked with zero-day attacks, and really sophisticated movement. Not so much that little edge stuff anymore.

**Kiran Mantha:**

If I can add to it, right, if you want to be the police - because you can't stop them from doing it on their mobile phone, right? But if you still want to do it, there is technology to engineer, right? So on the edge, there are vendors that actually have the proxies, you can configure them to filter for keywords, you can block certain things where the user actually goes in, it'll tell them: you're not authorized to go access this using your company resources. If you think this is an error, you can ask them to contact IT. So there are things you can do – technology exists for you to do it. But the question is, how far - how much do you want to police your people?

**Questions**:

You mentioned, one of our biggest threats, I believe, to most of us is insider threats, right? Our own employees. Can you refresh for us, what are actionable items that we can recommend to our staff in order to make them better aware, better equipped to protect our data?

**Kiran Mantha:**

Yeah, I'll start maybe, Todd, you can add to it. When I think of managing insider threat, I think you have to address it in multiple ways, right? First one is education. Everybody has a cyber program. But oftentimes what we see is it's once a year, check the box kind of thing. But how do you actually make it more meaningful for the user? Right?

**Kiran Mantha:**

So, we at Deloitte, we have this series called "Don't be that guy" series. (laughter) It's a quick, five-minute video that we do, with a scenario playing out, saying don't do it, right?

Don't be traveling in the elevator in – you know – the middle of 30 Rockefeller Center, and talk about your client getting breached, right? Little things that you do. So, thinking of innovative ways to educate users is probably important, right? The others - that takes care of sort of what I call people doing things without just knowing - like no malicious intent. The other side of it is people who actually have malicious intents. This is where you should have good controls, right? So, if your system administrators are leaving the company, you should have a process to rotate administrative privileges and credentials and things like that. So having some processes around elevated risk for key people is important. Right? And then the last piece - we talked about it, right - is this behavior based analysis. So, what we're seeing a lot of organizations embark on is what we call an insider threat management program. Right? So, it starts with the right policy. There's technology out there today that you can deploy, that starts observing user behavior and assigns a risk score to what the user is doing. And then it can take actions based on what you want to do, right. So, again, multiple ways of looking at it that starts with education, start with good processes and hygiene around things to do when key people leave the organization, and then of course, the broader program to catch all the pieces.

**Todd Knapp**:

So, I'm going to give you two terms that if you were going to write something down, write these down: least privileged access. Ask your IP departments what you're doing for least privileged access. The concept is that we don't assign privileges to the user that they don't need. And a lot of organizations, a lot of IT departments aren't that sophisticated yet. You may get a quick and somewhat glib response from an IT person saying, “oh, yeah, yeah, we never give people more than they need.” The next question is, well, then how do you monitor for privilege creep? Privilege creep, that's the term. So how do we know month over month that somebody hasn't added privileges to an account, maybe during testing and then didn't remove them? Or added them erroneously? That's the - managing identity is managing insider threat.

**Jason Kravitz**:

Under the - just the question, in terms of the legal aspect: Do we get involved - do the lawyers get involved in drafting the incident response plan, and then implementing it? So, the incident response plan is going to be different for every organization, but there are obviously going to be a lot of similarities. It just depends on how big your company is, right - how many departments, how many different people are going to be - or different touchpoints that you're going to have. But this is not rocket science, right. But it should be done by someone who is ultimately, like I said earlier, going to be the quarterback of the process, so that you just have this - it's a cheat sheet, right? Like, who does what, and what are their phone numbers? What are their email addresses? And it's just amazing when - because when the stuff hits the fan, as it will, inevitably, for some of you, it's just hard to stop the chaos, right? It is a very chaotic couple of days - you hope it's just a couple of days - when this thing surfaces, and you just want to have this cheat sheet so that you know: who am I supposed to call? And what are they going to do about it? Right?

**Heather Wilkerson**:

I think part of our discussion was really, too, like - help with the preparedness, right? If you're a very small business, if it's not your main business, you know, is there a set package to get this going?

**Todd Knapp:**

On that last subject, there: if you're part of a small business, and you're in a in a niche industry, talk to your industry associations. If you're a manufacturer, the Manufacturers Alliance has a program for small businesses that help them get through this. A lot of industry organizations have taken that path, because it's too hard for a small business to handle. So -

**Kiran Mantha**:

You know, I'll just add one last thing to this, right. As we think about an incident response plan, I always think about an incident commander. Think about who that is in your organization, because that can't be you. You're the CEO, and you still have to run the business. I've seen situations where CEO tends to become an incident commander, and that does not go well.

**Question**:

How do you measure how much internal resources versus external. External seems a little bit easier to me. So, maybe specifically, what kind of internal resources do you need as a medium sized business?

**Heather Wilkerson**:

Did everybody hear that? Talking about resources?

**Kiran Mantha**:

Are you talking about… Should we hire a whole security department internally or rely more on an external? And how do we kind of measure which? Yeah, I would say to that: it's, it's not about quantity. It's about quality, right?

I've seen security functions with as low as six, seven people run very smart, effective programs. And I've seen 30-40 plus people just sitting there warming benches, right. So, the question, I think, needs to be looked at: what are your priorities? What are you trying to tackle?

And how well you employ technology and automation to effectively do this, right? So, you know, I know I'm not answering the question straight. But what you need to look at is, what are the 5 to 10 things that we're going to focus on that's going to make sense for us? And what's the team that we need to do this right, right? And sometimes it means outsourcing some functions, right? Maybe outsourcing a full security operations to a third party helps you focus on something else, so - like identity management.

**Question**:

We had great conversations with lots of insights. One interesting question and perspective that came up has to do with the fact that, you know, we may have our own internal infrastructure, but in today's ecosystem, we rely on third parties, outside vendors, software as a service. And we shared that yeah, we have liability for that data as well. So, with that understanding, what guidance would you give everyone here around how to select - what to look out for when selecting those third party partners, and how often should we revisit that relationship to stay safe?

**Heather Wilkerson**:

Todd, why don't you start with that one -

**Todd Knapp:**

Why just because I smirked at it? No, I mean…

You know when there are… I tell people when they're searching for new software, there are four specific things that I look for in a new provider every time. And if they don't meet all four of these, they're not on my list, period. Don't look at it, no matter how good the workflow is.

Number one: identity integration - has to be able to take identity from my primary identity provider. If I'm a Google identity shop, then it's got to integrate with Google, if I'm a Microsoft shop, it's got to integrate with Microsoft. I don't take software that has its own username and password database. I just don't do it.

Number two: it has to be able to support data access - open data access - for analytics, and reporting. Number three: has to be able to support automation. Number four: has to integrate into whatever our primary communications platform is. If you're a Slack company, got to integrate with Slack. If you're in Teams, it needs to integrate with Teams. Those four things. If it doesn't do all four, don't even look at it.

**Jason Kravitz**:

Let me just make a quick follow up.

With respect to your contracts with your vendors, also, you want to be looking for an indemnification provisions, you want to make sure that - I mean the context - if you're doing anything that touches health care, the law requires you to have business associate agreements, right? So, this is this is not something to be taken lightly. Because if you don't do this stuff, the penalties are staggering. They are existential.

**Kiran Mantha**:

I'll add this, right - we always tell people: have a good third-party risk management program, right? So that goes from onboarding a third party to offboarding a third party, right? Because a lot of times, people take care of the onboarding right, they'll have the right contracts in place. They might even do the ongoing management. They might even do annual audits or just ask for stock reports, but a lot of times people don't do offboarding right. It's like, if you terminate a contract, how do you know that your data is still not out there? How do you know that they're actually living to their obligations, right? So have an entire program, end to end, and diligently following that up is important. Right? Now, all third parties are not the same. So, you have to think, based on risk tiering, what is high risk for you and probably have more scrutiny on them as opposed to others.