insideARM
Think Differently: TECH LOCK

Transcript of conversation between Stephanie Eidelman, CEO of The iA Institute
and Brian McManamon, President & CEO of TECH LOCK and Vice President of RevSpring
Published June 23, 2020

Stephanie Eidelman

Hi. I'm Stephanie Eidelman, CEO of insideARM and the iA Institute. I hope you are all safe and healthy. One of the things I spend a lot of my time on is managing our Innovation Council. Even before the pandemic, organizations in the Innovation Council understood that their ability to survive would depend on thinking differently and being at the forefront of communications, analytics, payments, and compliance technology. Last fall we started an article series called Thinking Differently, to feature thought leadership in these areas by our staff and by members of the Council. We've now expanded this series into video format, as I interview various members of the Council to share with you how they are thinking differently about their businesses, and about the future of the industry. I hope you'll listen in.

[Brief video animation introducing "Think Differently"]

I'm here today with Brian McManamon, president and CEO of TECH LOCK and vice president of RevSpring, and also a member of the Innovation Council. Brian, I've been looking forward to our conversation. So thanks very much for joining me today.

Brian McManamon

Thank you, Stephanie, for having me, I'm looking forward to it also.

Stephanie Eidelman

Great. Why don't we start with just a brief explanation of TECH LOCK. Who are your customers and what do you do?

Brian McManamon

TECH LOCK is a data security company. We are a wholly owned subsidiary of RevSpring, located out of, or headquartered out of Michigan. We do have a couple of remote offices about, 20 employees and growing, growing fast, hopefully. All of our customers are US-based. Our core industry segment is financial services. But we do serve other industry segments, including healthcare, manufacturing, energy, retail and hospitality. And, you know, really the vision of TECH LOCK is to help our clients be more secure by employing and implementing a turnkey, end-to-end managed security and compliance solution. And it's really to address, if you think about compliance, all the different standards that impact our, our industry. So PCI, HIPAA, ISO 27,001, SOC 2, HITRUST if you're dealing with healthcare collections.

Brian McManamon

So all those different standards and there's really two sides to our business. There's a consulting side to the business, where we do auditing and penetration testing against all the different standards that I mentioned. And then I'm happy to announce we're launching the second side of our business, which is our managed security services offering. And I'm really excited about that side of our business. What that is, is we've partnered with some of the best security products that are out there in the landscape, and we're offering a holistic solution end-to-end, as I mentioned before, turnkey, with solutions for endpoint protection that incorporates next generation and antivirus technology with behavioral and machine learning to secure against threats, log management, firewall and network management, vulnerability management, compliance, maintenance, and then what I call an integrated assessment.

So a lot of different buzzwords there, somewhat technical, but we're really proud about that because again, it takes that holistic approach. It integrates security, but with a compliance perspective on that security. So all of our solutions that we implement, we make sure that our customers stay compliant. We are orchestrating all this security data, powering it through a machine learning engine, and then we're monitoring it 24 by 7 by 365 with our security operation center. We're guaranteeing all of our services through a service level agreement with a 15-minute response time. And then we're supporting it through a customer portal with complete visibility and transparency. So our clients have real time data and information as to what we're doing with our service.

Stephanie Eidelman

Interesting. You mentioned the machine learning aspect to it. What kind of information is that?

Brian McManamon

Yeah, you know, we're really proud about that. We are totally cloud-based. So we take all that data through the cloud. And what we're trying to do is really focus on the security events that matter. So as you could imagine, there's a lot of noise that happens out there in the wild and what that machine learning engine does is it pays attention to that noise. And through algorithms, tries to weed out that noise and only focus on the events so we can get to the response faster through our security operations center. Otherwise, you know, the threat could stay out there. You know, if you're talking about thousands and thousands of security events that may be happening at any point in time, it may be the one to five events that really matter that you have to respond to very quickly, before that threat causes damage within a customer's environment.

Stephanie Eidelman

That makes sense, and so your system would help raise those to the top so you address them first. And I suspect that the new environment that so many are working with that have worked from home, which brings really new challenges at least to the collections industry that maybe they didn't have before, as it relates to security. Is that something you're spending a lot of time figuring out?

Brian McManamon

Yeah, it is. Luckily we had a head start on that, but with all the work from home and a lot of our customers as you've probably heard before everybody scrambled and the first probably month they deployed the work from home solutions, there are a lot of changes that occurred within our customers' environments. So what we try to do is make sure that we work with them to make sure that any changes that they made kept their environment secure, as well as some of the solutions and services that I just talked about. If you think about that end point, you've now opened up the risk on those end points. Because you're not always sure what those agents or what our customers' employees are working off of, what they have access to. You've just expanded that threat landscape. So we're helping our clients deal with that. You know, other clients looked further into how they're deploying those technologies. So they may be deploying thin clients or remote desktops, requiring two factor authentication, which is best practice, and really making sure that they had the right solutions in place to provide that extra security.

Stephanie Eidelman

Yeah. As you see what's changing and some changes are perhaps temporary, but others are expected to be more permanent, how are you thinking differently about your business and where you need to be positioned in the future?

Brian McManamon

Yeah. And you know, I think we're trying to figure out, for example, on the compliance side. You know, there has been a lot less travel. So for customers that have to maintain compliance with PCI or other standards, whether it's HITRUST, again for healthcare, or SOC 2, how do we accomplish our audits and provide our services remotely? That's definitely a difference than what we've seen in the past. Because we can't travel, we can't collect our evidence onsite any longer. We have to do all that remotely. So how we interact with our customers to make that happen has definitely been a different challenge that we haven't had in the past. You know, on the managed services or managed security services side, it's definitely been a difference in trying to help our clients think differently because again, the threat landscape has changed.

So for example, you know, with COVID-19, we've seen a lot of threats out there in the wild, related to phishing attacks. You know, a lot coming through email and depending on what those agents are or our customers' employees, depending on the industry, what they're susceptible to, you know, you have to be aware of with additional training, what those employees may be clicking on, and then provide that proactive protection in the background. So that's where we try to really focus some of our services that I talked about earlier. So for example, one of our solutions is endpoint protection. So even if you're not able to stop that email before it gets to that employee, if they do click on that link, how do you provide that additional layer of protection, and with our end point protection solution with that next generation antivirus, we've never had, for example, a successful ransomware attack, because it's able to identify those types of attacks and head them off at the pass, so to speak.

Stephanie Eidelman

Yeah. Is there a different way that you need to even deploy your solutions? You mentioned a different way of auditing because you can't do in person, does the same corollary apply to the software?

Brian McManamon

Yeah, it absolutely does. So one of the advantages of our solution is that it is cloud based. So now you've got to think about, if you're not deploying solutions like thin clients or remote desktops where you're executing applications off the server. You've got to think about if there is a deployment of software on the end user's machine, who's working remote, how do we do that? How do we protect that? We've deployed cloud based solutions so it doesn't matter that they're not, or potentially on your network, you still maintain that protection because that cloud-based agent is always there, always running, always providing them that additional layer of protection.

Stephanie Eidelman

Is there a particular concern that's keeping you up at night these days, the most?

Brian McManamon

There is. Because we run a 24/7 security operation center, I like to be very involved in what's happening with that center. So, you know, there's constant messaging going back and forth about security events that are happening. So we get very involved in that. As I mentioned, there's a lot of interaction with the team to make sure we're staying on top of those, you know, hackers aren't sleeping, right. And a lot of that activity is happening during off hours. So, you know, we're trying to protect against that. Our customers' data and protection of that data is our number one objective. You know, what we're seeing too, as I mentioned earlier in the interview, customers' resources are shrinking and the longer this pandemic goes on the more risk there is. So we're trying to fill in those gaps and know where customers are trying to save costs. We're trying to provide the additional layer of efficiencies, as we fill in those gaps. So we can help our customers operate more efficiently.

Stephanie Eidelman

One other question that I thought was worth visiting, we talked about it before we started the official interview was how some of your clients you've seen successfully changing their business to stay afloat during this time. What are some of those success stories that you've seen?

Brian McManamon

Yeah, there's really two things that come to mind. One is some of our customers, especially ones who are running call centers have looked for alternative use cases for those call centers. So for example, since the collections activity has been reduced or eliminated almost during this pandemic, what are the uses are there for those agents to fill the gaps? So one of them is for example, customer care type initiatives, and certainly, related to the pandemic. So maybe providing government support is one of the use cases that I've heard about. So really redeploying those agents to do other things. That and shifting their business model. The other thing that's been very interesting that's come into play is with agents working from home, how do you protect the data? So if they're receiving calls and taking credit card information, how do you protect that information?

So I know for example, talking about RevSpring. RevSpring does that through self-service type activities where the agent is not involved at all and receiving that credit card, it may be taken via a payment portal or via an IVR interaction. But if they are taking it through our client's application, that certainly adds a level of risk that needs to be understood, right? Because that agent could be writing down that information, for example. So that's something that we've had some conversations with our customers about how to reduce that risk

Stephanie Eidelman

Of the clients that have deployed the self-service payment options, have they seen a drop or an increase in how many payments actually get made? You know, are they losing any sort of in the translation?

Brian McManamon

Sure. No, I actually, I think that it's made those clients more efficient. Normally we do see an uptick and working with those clients on how they collect those payments, if it is via self service. You know, a lot of times customers, or consumers, want to interact that way anyway. They would just love to get it done versus talking to an agent.

Stephanie Eidelman

Yeah. Or for privacy reasons, they feel, that to protect the security of their information...

Brian McManamon

Security of the information. And, again, you know, from our customers' perspective, you’re talking about efficiencies. It's more efficient, right?

Stephanie Eidelman

Definitely. And less opportunity for error. If they're calling out a card number and you have to type it in, some percentage of those entries are going to be wrong.

Brian McManamon

Absolutely.

Stephanie Eidelman

Well, wonderful. I really appreciate your time today. This was, I think, really helpful, and I look forward to continuing the conversation with you at our Innovation Council meetings.

Brian McManamon

Sounds great, thank you.