Solving the Remote Work Cybersecurity Conundrum

Welcome to Digital aspirations from Aspire technology partners, a podcast series where we discuss technology insights, driving today's business transformation. This podcast is sponsored by Cisco. Aspire Technology Partners is a leading systems integrator and Cisco Gold Certified Partner.

Doug Stevens: So, today we're going to talk about the current state of cybersecurity landscape and what organizations can do to protect themselves. And I'm excited to be joined by two guests today who will share their insights and experience in the security space and, hopefully, provide actionable advice that our listeners can take away to advance your organization's overall security maturity.

So, our first guest today is John Rossiter. John's a Principal Consulting Engineer and the Chief Information Security Officer for Aspire. John also leads the team that develops and manages the technology stack and the platforms that support our security operations center. So, John, welcome.

John Rossiter: Thank you, Doug. Great to be here.

DS: And our second guest is Michael O'Connell, and some of you might recognize that name. Michael is becoming a regular on this podcast series. If you're not familiar with Michael, he's a Solutions Architect within our Cybersecurity Practice Area. He brings a ton of experience. Mike has over 15 plus years of experience designing and implementing security solutions. So, Mike, welcome again.

Michael O'Connell: Thank you. I'm glad to be back.

DS: All right. So, what I thought I'd do to kick things off is to share what I thought was some interesting research that I read recently, and it comes from a survey from PWC. And, essentially, it talked about 64 percent of CISOs and CIOs expect to jump in reportable ransomware and software supply chain incidents in the second half of 2021. Now, that in it of itself isn't very surprising. We've seen those numbers jump pretty dramatically and continue to.

But it was interesting that the reasoning behind that was this notion that, as organizations rust to adapt to the pandemic driven challenges, and work, and business models, in many cases, security got left behind. And over half of those surveyed felt that they hadn't adequately addressed the risks associated with remote workers, digitization, and cloud adoption.

I mean, when we talk about work from home, that literally happened overnight. COVID hit, everybody worked from home, and securing that remote workforce is still in catch-up mode. I mean, at that point, that back in March a year ago, 70 percent of organizations were still relying on password-centric authentication. So, that was a major factor.

Another factor is a lot of that work from home motion pushed the network edge to include, really, common home devices. We have people connecting to the office with a home device. Not hardened, nowhere near the same degree of security that you'd see on a corporate device. And then, we also know that the vast majority of data breaches today involve some sort of human element. Somebody is unwittingly clicking on something or there's some sort of social engineering or phishing associated with these breaches. So, that all contributed to a vastly different threat landscape.

In terms of digitalization and business transformation, the speed at which these companies leverage, DevOps, and AI, and ML, and some other technologies, to transform their business models really created some additional security challenges there. And the question becomes, how do organizations strike the right balance between speed to market and agility versus privacy and security.

And cloud security was another concern. We saw a significant increase in the pace of cloud adoption. And over half of the companies surveyed said that they weren't actually getting the full value of the cloud. And the reason being is, they failed to take into account the unique security challenges that the cloud adoption poses or at least they didn't address them early enough in that process.

So, to me, it was interesting to understand the effect that this global pandemic had on businesses and the challenges that it presented to both IT and business leaders, who, in many cases, are still dealing with this today, 18 months later. So, again, I thought that was interesting backdrop. I'm certainly interested in your thoughts as well. Michael, I'll throw it to you first. How would you describe the current cybersecurity and threat landscape today?

MO'C: So, the biggest difference is to talk about the different verticals between cybersecurity and threat landscape. So, one example would be healthcare. So, in healthcare, one of the biggest issues you're currently looking at is ransomware, and that can affect in three ways. So, a phishing email schema, a user clicking a malicious link, or any kind of advertising or malvertizing, they call it.

One of the biggest things in the healthcare industry, critical processes are slowed down or become completely inoperable. And hospitals are forced to go back to utilizing pen and paper, slowing every individual process in that medical facility. And, ultimately, soaking up funds that may have otherwise been allocated for automation in today's dynamic workplace.

That same thing can be said for any industry, whether that's educational, financial, manufacturing. Automated processes are eliminated with the current cybersecurity threat landscape that we see in the news and on a daily basis.

DS: Exactly. It's a huge challenge for, not only healthcare, but across multiple verticals today. John, I mentioned remote workers and digitization and cloud adoption in the opening there. What are the other security challenges that organizations are facing today?

JR: That's a great question, Doug. We've got quite a view of a few of those challenges that you're going to see. Number one being legacy infrastructure. Being able to upgrade potential infrastructure to meet the demands of work-from-home have been exceedingly difficult for most organizations. So, obviously, budgets are strained. COVID has adversely affected most of the companies that we have worked with. They haven't been used to or they just got immediately thrust upon them the work-from-home motto. So, from there, very difficult without the proper tools being able to, all of a sudden, IT now has to take care of all these devices that they may or may not have direct control or access over.

DS: So, I want to open this next question up to both of you, and knowing what you do on a daily basis and the number of clients that you speak to on a regular basis, given some of those challenges that you mentioned, John, and the threat landscape, what are the trends that you're seeing? What kinds of security initiatives are organizations undertaking to protect themselves?

MO'C: So, one thing that I see on a daily basis is the need to adopt a multiplatform approach or cloud-based product from managing anyone no matter where they're at. So, whether they're home, whether they're traveling, whether they're in the office, the need has been proven. Especially, as John mentioned, with COVID, with the legacy landscapes, to adopt and move to a cloud-based single platform solution where you can manage your users and organization's devices no matter where they're at. You need the enforcement to be able to put an additional layer of security. And gone are the days where someone's only in your office. So, no matter where someone's at, we need the ability to protect the corporate assets.

DS: Cloud is huge. I agree. I mean, managing complexity, taking complexity out of the implementation process, being able to manage remote sites and users with common policy, all those things have been a huge benefit derived from the cloud. John, any thoughts there on trends that you're seeing?

JR: We're also seeing the concept of zero trust. It's actually been around for quite some time. But we're starting to see organizations take it a lot more seriously. And, essentially, what that is, is just really giving the minimal amount of access that is necessary to do or perform one's job. So, it sounds simple in concept, I should say, but it's quite a difficult thing sometimes to achieve within an organization throughout legacy infrastructure as well. So, it's definitely one of those things that a lot of our customers are looking to do and embark upon.

DS: And I think that that framework itself, if you drill into it a little bit, it would seem to address many of those challenge that we mentioned earlier, so securing remote workers and hybrid cloud environments and protecting against ransomware threats. Michael, if folks out there aren't familiar with zero trust, can you explain to to our listeners what zero trust is? And I'd be interested from both you as well, is it viable? Is it even realistic for, say, a mid-sized organization to be able to adopt?

MO'C: Sure. So, the principles behind zero trust is that you assume that attackers are both within and outside of your corporate network. So, no user's machines should be automatically trusted. So, in legacy infrastructures, if someone had a machine, for example, a desktop in the organization, automatically that was trusted. With the zero trust model, you're assuming that whether that's internally or externally, it's malicious or nontrusted until proven otherwise.

There's a couple in depth ways you can go about that. So, from an adoption or a viable or realistic approach with organizations, yes, it's a feasible way and you can automate visibility and trust verification in the organizations. I'll let John go in a little more details with that. But, yes, I do believe that it's a viable and realistic approach. I think there's a multi-step process to get there. One of it being devices, user authentication, for example, two-factor, but I'll let John go in a little more detail. But to answer your question, the bottom line is, it's the philosophy that nothing's trusted until proven otherwise.

DS: So, it's the opposite of our legal system here in the United States. It's an all users are guilty until proven innocent. Is that what you're saying?

MO'C: Correct. Correct.

DS: Okay. John, what are your thoughts on zero trust and its feasibility in midsized organizations?

JR: Definitely we get a lot of pushback when we first introduced some of these ideas to customers. But, really, in principle, you don't have to boil the ocean. So, you can start small and then progressively add to your zero trust infrastructure. So, you can start with your applications. Certainly, a lot of customers will go ahead and start with their SAS based applications. Go ahead and implement zero trust principles there along with some of the products that such is two-factor. Start low and then as the entire user community gets more comfortable with the idea, then you go ahead and introduce those in the internal and legacy networks as well.

DS: Okay. And what are some of those technologies? I mean, we don't want to get into products here. We're product agnostic here. But what are some of those technologies? You mentioned multifactor.

JR: I mean, there are a lot of different products out there from a lot of different vendors. We do utilize Cisco Duo quite often for that. We also utilize OCTA for that infrastructure as well. And then, once you go ahead and look at providing zero trust or doing zero trust on your infrastructure, Cisco ISE is probably our primary product that we would use to achieve that.

DS: Mike, any thoughts there and advice?

MO'C: Absolutely. So, just as John just mentioned, when you're looking at your network and your endpoints and the trust viability inside the interconnectivity, ISE for example, but any network access control solution. So, you want to make sure that you have the device and the user and the data is all verified and controllable through automated visibility and trust verification.

DS: So, it's a journey it sounds like. Trust, it's not something that you're just going to snap on overnight. It's something that can be planned and implemented over a period of time. And it sounds like it's achievable.

JR: Absolutely. A little bit at a time. [Inaudible].

MO'C: Exactly what John said, a little bit step by step.

DS: Okay. Perfect. All right. Well then, that sort of leads me into my next question, and that is, as companies are implementing some of these security controls relating to zero trust or just security in general - and, John, I'll direct this towards you - we know that it's extremely important to recognize that having tools in place is really only part of that equation. Can you talk to your experiences and the importance of being able to monitor security events in some meaningful and consistent way?

JR: Sure. I mean, we get this quite a bit when we talk to our customers who've actually invested in the tools. And so, what I mean by tools are endpoint protection, potentially, DNS, network traffic analytics, next-generation firewall, IPS. So, they have a number of these different tools at every point of their network and in the cloud. But one of the big biggest pieces of the puzzle that they're missing in a lot of cases is that know-how to look at the invents that are coming from these devices or these solutions.

So, there's a comfort level, I guess, when you go ahead and purchase these tools, and it may be misplaced. So, the tools will definitely tell you what's actually happening. But a lot of times they're not a hundred percent, and so you need to have multiple tools in order to pick up for where one, a little bit, may have missed something. But either way, having somebody who is qualified to actually look at the events and understands those events that are in there, not to mention the folks to actually tune those tools and take care of them, a really important aspect of making those tools successful.

We've had a lot of customers sign on to our service after they've had security events, even though they've had the tools. And, again, the missing component is having somebody eyes on glass 24/7 with specific know-how with these tools. So, we specially see this in the mid-market. So, we have a lot of folks wearing multiple hats and, certainly, they're not available on 24 by 7 fashion, nor do they want to be.

So, I mean, that would be the tagline here, Doug, is that, the tools are really important but just as important are the folks looking at those tools.

DS: For sure. And having the skillset to be able to understand and react to those alerts in some sort of real-time way. And the reality is, mid-sized companies it's hard to find those people. There's a fairly large investment to build the platforms, and buy the sim, and have the multiple shifts, and whatnot. So, the best option there for many of those sized organizations is to engage in MSSP partner, and outsource that, and find a good one that can really be an extension to your IT team.

So, we're just about out of time. But before we break, I did want to give John and Michael an opportunity. Any closing thoughts or any advice that you can share with our listeners to help them as they go down that journey to protecting their businesses?

MO'C: think one of the things to look at, as you mentioned, John and Doug, it's very important and focused on if you're looking in and adopting a zero trust, it is feasible, it's viable. But you need to manage and work with someone that knows the tools, like John mentioned. I think that's extremely important. And you do it in a phased approach. That's the only thoughts or advice to just wrap this up from my side.

DS: Great. John, any closing thoughts?

JR: Sure. I mean, we've talked a little bit about tools, about some of the things that we're seeing in the threat landscape, but, really, there's no two ways of going about and actually putting together a solid security program for your organization to ensure, number one, that you have the proper policies in place along with those tools that are protecting the environment and the correct personnel to monitor that environment. So, it's really important.

Doug, your point earlier, most of the attacks that are occurring are really targeted towards the user. So, along with a good security program, the policy and the rules, you really need to make sure that your users are in the know. So, we also, as an organization, really highly recommend that part of any good security program is going to really be inclusive of your users and making sure that you've got regular training for those folks. They are your key to success there, or your failure, unfortunately.

DS: In many ways it could be your last line of defense is your user population. And a great point, security awareness training should never be overlooked. It's extremely important. So, that's all the time we have today. Thank you both for sharing your knowledge and expertise. I really appreciate you both being with us today.

To our listeners, if you like the discussion today and you'd like to hear more podcasts, go to our website, aspiretransforms.com. And as always, thank you for listening and we'll see you next time on Digital Aspirations for Business. I'm your host, Doug Stevens. Bye for now.

Digital Aspirations is brought to you by Aspire Technology Partners, a premier technology solutions and services provider designing, implementing, delivering, and managing digital infrastructure and IoT solutions to enable transformational business outcomes, creating more agile and efficient IT environments that deliver differentiated customer experiences for your organization. To learn more about Aspire Technology Partners, visit aspiretransforms.com or email us at podcast@aspiretransforms.com.

cisco
Partner
Master Collaboration Specialized
Master Networking Specialized
Master Security Specialized
Gold Integrator

Aspire Technology Partners is a Cisco Gold Certified Partner engrained in solution pillars that set us apart as a true Cisco solutions provider. We are committed to the continuous improvement of expertise and skillsets around Cisco initiatives that enable us to help and guide customers in the adoption and management of technology architectures designed to transform their organization. We hold Cisco Master Specializations in Collaboration, Security, Cloud & Managed Services and is one of only 25 partners in the US to receive the Cisco Advanced Customer Experience Specialization.