Aspire Technology Partners - The Digital Aspirations Business Podcast – Series 1, Episode 2, Part 2

Top IT Priorities for 2020

Doug Stevens, Vice President for Managed Services, Aspire Technology Partners
John Cope, Regional Technology Solutions Director, Aspire Technology Partners

Doug Stevens (DS): Hello. Welcome to Episode 2 of the Digital Aspirations Podcast Series. My name is Doug Stevens, and I'll be your host.

Our topic today is Top IT Priorities for 2020, and this is part two of a two-part series. If you missed part one of the podcast, you can find it at our website, AspireTransforms.com.

Joining me today for part two is John Cope. Johnis our Regional Technology Director for Aspire. He's based in our Albany office. John, welcome.

John Cope (JC): Thank you, Doug. Glad to be here.

DS: In addition to serving in the military, which we all thank you for your service, give us a little more background about your IT industry experience, if you would.

JC: So, I started my IT career with a tier one service provider early in the late '90s-2000. Pretty much, if you had a pulse, you could get a job in IT. I started building out the tier one internet service with a company called Cable & Wireless. I absolutely love that part of my career because it gave me exposure to multiple technologies all at one time. There was a lot of market fragmentation back then. We got to dabble in everything from the Cabletrons of the world, to the Foundries, to Cisco. From a security perspective, the Junipers. All of it all at one time.

I moved on from there and became a network designer for Boeing Company. There, I was chiefly responsible for our voice implementation, which, at the time, was about 100,000 devices on the Cisco Call Manager. At that point, I believe we were adopting version 3.3. So, we were early on into that

program, and we cut our teeth on it, and basically moved Boeing along, which was monumental to Cisco back then.

After that stint at Boeing, my lovely wife decided she wanted to come back home to Upstate New York, and she suggested that I should follow if I wanted to see my children again. So, I took her advice. We came up here, and I did a short stint with some of the financial markets where I got to build out some unique and interesting solutions around Bloomberg, Brass, and ringdowns that we were using at our desks, and moving all those to IP for the turret systems.

And then I moved on from there to Tandberg where I did a lot of the video conferencing type of integrations and moving that convergence of video into the IP telephony platform. And then, as everyone knows, they were acquired by Cisco later. My Cisco career was about 12 years. I started off as an SE and then moved up to an SEM. Eventually, I took on the region manager position. And then, after that, I jumped over here to Aspire to help build out a practice in the Upstate New York arena.

DS: And the rest is history, as they say.

JC: The rest is history. That was a long introduction, but just to give you some of the background.

DS: We're happy to have you. Great experience, obviously. Service provider of large enterprise and financial services. And then, of course, leadership roles at Cisco. Thank you for being with us today. Before we jump in though, I do want to remind our listeners that, in part one, we covered three IT priorities with Kevin Lehey.

The first one we talked about was ransomware and the fact that data protection has really moved to the boardroom and become a C-level concern. The second priority was about cloud scaling, and integration, and the challenges in early workload decisions for cloud deployments.

And then, the last priority that we covered was around internal IT management processes and making sure that IT isn't holding back the pace of transformation. It was a great discussion. I'm sure we'll have a ton of valuable insight from you today in part two. So, let's get started.

JC: I'm excited.

DS: Goosebumps, right? Here we go.

Leverage Data to Gain Greater Insights

We are in the year 2020, obviously, and I heard somebody refer to 2020 as the beginning of the data decade. It's the first time I heard that, but it's so true. Data analytics and the enabling technologies like machine learning and artificial intelligence have experienced a maturity process. Businesses use that data to take actions and make meaningful decisions. Our first IT priority for 2020 involves leveraging IoT data to gain greater insights.

John, what do you see in terms of a trend for IoT-driven data? And what is the potential impact on our daily lives?

JC: The impact on our lives is around these data models that we need to create. We talked about 2020 being the data decade, but data has been around for a very long time—we're just now starting to glean some of these insights from it. That starts with the first step of realizing that not all data has value. We started down this realm ten years ago, and we collected a lot of data, but we are just now starting to get into that model where we've got to ascertain which data truly has value. If you look at the trend around it, we've gathered a lot of big data, but that's also been the bottleneck.

I've been to a number of customers, and they build out these massive infrastructures around big data, and they have petabytes of this stuff sitting around, but those petabytes of data have created the problem of being able to analyze it. The better approach to this, in the world of IoT, is to state the problem, which is similar in business. Think about what problem you are trying to solve first, not just collecting data for data's sake, but defining that problem statement. This will allow you to develop the right data model first, and then articulate which data points you have that will help you solve [the problem while being able to correlate to solve your problem that you define.

We also need to realize that data has a different value as it relates to time. It's like the time value of money in business. The data models that produce real-time, or near real-time, or historical results each have different value in the stream and should help derive the problem statement.

As far as the impact on some of our daily lives, there's an interesting book about this. The book is called *Abundance*. It's based on the premise that the problems of the future are so big and massive that the only way that we can solve them is through technology because of resource constraints. I absolutely agree. The problems of today and tomorrow are massive as it relates to energy management, waste

management, safety, and security. And the more insights that we can derive and obtain through the data, the better solution we'll have.

So, when we talk about narrowing that down to the impact on our lives, everyone is a part of this. I mean, you can't even go to Home Depot anymore and buy a device that doesn't want to talk or give up some data to some service. All of this is done around automation and with the purpose of making our lives easier, but its impact also relates to how we even think about solving the next problems that we are ascertaining. A big one in the industry is safety and security. You have a lot of organizations that are trying to drive that particular issue in the market, and we have to solve that problemwith data.

DS: I totally agree. What you said earlier about defining the problem and then trying to solve it is key because this can go in so many different directions and could be overwhelming. Like what you said around safety and security: we've seen use cases with some of our existing customers around things as simple as, "Hey, when is the waste paper basket full in an airport bathroom, and how do we make sure that the user experience is what we wanted to be when folks are traveling?"

JC: And to that point: I'm working with a customer around vehicle safety as they traverse the roadways. There's very interesting technology when we talk about the vehicles we drive, whether it's DSRC or cellular. These vehicles are spewing out data. The traditional way of collecting [the data along roadways] had been parks and local loops—even some of the data that comes from toll plazas, but it becomes challenging from an operational perspective.

As we move forward, we'll design the features to use the devices themselves as sensors. Let's listen to this vehicle data, but let's develop the right data model first. For this project now, we have five different use cases. I won't go through all five, but the first one is around work-zone safety. If we can use the vehicles as a sensor to take in information such as speed as cars approach work-zones, and then change signage dynamically based on the data feed, we're defining the data model for the relevant pieces of data that solve the problem around work-zone safety. We can get rid of the data without value at the point in time, and we can classify the valuable data in near real-time. If we want to produce historical results over that data to test and validate our models, we'll store the pieces that have different value for the historical pieces. It's a different way of approaching data instead of throwing devices to suck-in all that data everywhere.

Keeping Up with the Pace of New Cybersecurity Threats

DS: Priority number two is around security, but it's more than just ransomware. The threat landscape is continuing to evolve the nature of business today. The attack surface continues to widen. New attack vectors continue to emerge. There's a much bigger picture here. The second IT priority for 2020 from our perspective is keeping up with the pace of new cybersecurity threats. What are you seeing and how should organizations be addressing this challenge?

JC: This is a very interesting one, and it's a problem that everyone's trying to solve. I do a lot of the cybersecurity in the Air Force, and I'd say we got a pretty good handle on it, but we fight this every day as well.

The security problem relates to the first priority around data. Security is a data problem in its very essence. Our customers experience what we've talked about within the big data realm because they got all kinds of security products that are feeding data, but it's also been exacerbated by a fragmented market. The fragmentation has created an interesting paradox of choice, which has stalled the market or led to customers reverting to the way they did security yesterday. Although the security problem looks insurmountable, it's about realizing that, at some point, you're going to get compromised, and you need to move to how you can contain it.

And so, if you look at the world we're living in today with all the recent announcements with the coronavirus and things of that nature, there's a lot of similarities to how you can attack your logical or your digital security. It's no longer really around prevention; although, it must be a part of your strategy. Don’t try to be the best. Try to improve every day.

Identify the data sets first because when you identify which data has value, which is what we talked about in that first statement, we can limit the attack vectors, or the compromises, around that data where we're no longer only drawing a line in the sand and saying, "All right, here's my firewall. This is my side. This is your side." We need to decide which data is valuable. Once we determine the valuable data, we can assess the state of the valuable data. Finally, we can implement a security strategy to protect the data in the various forms.

Thus, it becomes important to realize that you can't do this alone anymore. Security professionals need to focus on assessing the value of their customers’ data. Next, the security professionals should outsource the day-to-day monitoring of your policy. Security professionals should identify the data,

define the security posture and policies they want, and outsource some of the monitoring of those policies. Case in point: our Managed Security Services offering.

Security's also a big data type of problem. Artificial Intelligence must have a role. When you look at the various security players in the marketplace, you need to double down on those vendors and manufacturers, which we've brought into our portfolio, that are doubling down on that AI piece because you've got to apply some degrees of machine learning into this problem; you've got to be able to automate that because security has to be the same thing we talked about, and I need to act in a more real-time or near real-time basis.

Everything returns back to the paradigm: identify, prevent, isolate, contain, and then remediate. Once we put our data in these sets, and break it down into those categories as we put the right pieces and parts that give you a holistic view of this, we will take steps every day to re-evaluate what we've done because you constantly need to re-evaluate past processes. The threat landscape is constantly changing.

DS: I totally agree. Everything you said there is certainly near and dear to what we do for our day jobs here. So, yes, there was a couple of interesting points there. One is getting better from a security perspective; from a security and risk management perspective, getting more mature is key. Another great point is prioritizing risk and understanding what your most valuable data sets are and adding in the protection around those data sets.

Outsourcing has become a real need because of the lack of trained security resources out there. The other piece to that too is what you referred to earlier: the automation piece. There's so much data coming out of these logs from these various security controls that, unless you're looking at it in real time and reacting to those feeds, you're not getting the true value of the investment in your infrastructure. So, I think, everything you said there certainly hits the mark.

Just one other comment from my perspective is that all this ransomware, and all this awareness around security, is a byproduct of security being in the news on a regular basis. So, if there's any positive that's come out of this is that, I think, from the end user perspective, there's much more security awareness around how to treat questionable looking emails and things like that. What do you think?

JC: I think everyone has realized that security, from a cyber perspective, has to be part of their daily lives. Because it hits home now. You have the same adoption because it's loosely been consumerized. It used to be the big business piece and the biggest concern for businesses. People are now taking their

security practices home with them because they also have lots of data. They have all these devices coming on their home networks, and so it started to hit home. People started to pay attention.

DS: Yes, no doubt, because of the fact that phishing activities and some of these other threats are all email-born, and the attack vector is social engineering.

JC: The number one attack vector is email.

DS: Awareness of the threats and the vectors are key.

The Impact of the Collaboration Experience on User Efficiency and Employee Retention

DS: IT priority number three relates to the digital workspace. The digital workplace refers to a concept where organizations are creating workspaces to enhance the overall employee experience. A big piece of that is the collaboration experience, specifically how users interact both internally and externally, and creating ways to make it easier and more intuitive for users to do their jobs. It's funny because six or eight years ago, BYOD was the big challenge and the problem you're trying to solve there is "Hey, how can our users use their personal devices?" And it seems so long ago. It's not even an issue anymore. After that it was more about tighter integration of our collaboration tools with the office applications that we use daily as well as increasing productivity. But this space is moving so quickly and progressing so fast that now it's really about the impact that the collaboration experience has on user efficiency and employee retention. What are your thoughts there?

JC: I would say one of the big ones is retention and recruiting. We work differently nowadays. The next generation will work entirely differently than we do. And case in point, my daughter recently worked on a paper. For research, she used the social media platforms she likes to use, and she gained a ton of input from various sources. She used the input to frame her paper. I remember, when I'd get an assignment, I'd go home, and I'd work on it in my bubble, and I would come back and get that result.

When you look at companies, they've got to enable this type of working environment because this is an example of the way that the next generation wants to work - collaborate. If you want to recruit and retain top talent, you've got to enable these different ways that people collaborate, because, if you don't, it will impact the company's ability to innovate in the arenas where they play, and it will impact the bottom line. When you look at the organizations today, there are many that are entirely changing the physical workspace along with their collaboration tools to foster this collaboration.

DS: No doubt, no doubt. And it's moving quickly, as I said earlier. It's not just how they work, it's where they work too. I just read a Gartner survey recently. The survey respondents were asked: what proportion of your time would you like to spend in the corporate office, working in a public space like a coffee shop, working from home, communicating while traveling? They broke out the survey results by millennials and all these different age groups. I think that the goal there is to develop these personas. You talked earlier about identifying the problem, and then creating the solutions. The same concept is here. Create these personas of how people want to work, and then develop the collaboration experience to meet those needs.

JC: 100 percent. And then, obviously, wrapping into these collaboration portfolios what you need from a data protection and intellectual property perspective because the other thing is that, if you don't, people are going to use the tools that are available. They find ways to solve their problems. I mean, we're all creative. If you don't give them the tools and make it easy, then they're going to use the tools that already exist from various SaaS providers that might not follow your security paradigm or your posture.

DS: I totally agree. There's a bunch more of innovation happening in this area too: things like virtual personal assistants, leveraging ML, and some of the natural language processing, to Siri-like behavior. I can say, "Hey, personal assistant, add a meeting to my calendar and invite JC." Those types of things are coming and it's incredible.

JC: The AI in this space has truly been amazing. I recently went to a presentation. Two very large manufacturers partnered together from an AI perspective. One made an amazing collaboration package. The other added the AI piece to it. Those two together were very interesting because, we're talking about being able to do things in real time and solve some of the problems have really been in this industry. I immediately thought of a use case around this: virtual hearings. There's a lot of organizations moving to duplicating their physical space in the virtual realm. This lends itself to being able to do translation services on the fly.

DS: Everything that you've talked about in terms of the advancements around the collaboration experience can easily impact an organization's ability to attract and retain top talent. There's a ton here to chew on. We could probably do a future podcast on this topic alone. So, let's find time to do it. But, unfortunately, that's all the time we have today. Before we go, let me just recap what we talked about. The top IT priorities for 2020 here in part two of our podcast were:

1. Leveraging IoT data for greater insights
2. Keeping up with the pace of new cybersecurity threats
3. The impacts of the collaboration experience on efficiency and employee retention.

So, John, before we break here, any closing thoughts?

JC: The biggest one that I would just close with, because it hits on each one of these, is: define your problem and define which data sets will solve your problem, so that you can get that data model developed first. Remember: not all data has value. Define where the data has value, and whether you need the data in real-time, near real-time, or historical time.

DS: Awesome. I'm going to get a tattoo. It's going to say, "Define your problem; solve the problem." So, good words. Thank you for sharing your perspective. I really appreciate you being with us today. And again, just for the listeners, if you missed part 1 of the Top Priorities for 2020 Podcast, you visit our website, AspireTransforms.com. As always, we thank you for listening, and we'll see you next time on Digital Aspirations. I'm your host, Doug Stevens. Bye for now.

Cisco Partner
Gold Certified

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.