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

Top IT Priorities for 2020

Doug Stevens, Vice President for Managed Services, Aspire Technology Partners

Kevin Leahy, Data Center Practice Director, Aspire Technology Partners

Doug Stevens (DS): Welcome to episode one of The Digital Aspirations podcast series. My name is Doug Stevens and I am your host. If you like what you hear today, go to aspiretransforms.com. There, you can watch one of our Techcast webinars, read our Aspire blogs, and by all means, please follow us on Twitter.

Our topic for today's podcast centers around the top IT priorities for 2020. This is part one of a two-part series. Joining me for part one of the podcast is Kevin Leahy. Kevin leads Aspire's cloud and data center practice. Welcome, Kevin.

Kevin Leahy (KL): Thank you.

DS: All right. Now, at the risk of making me sound old, you've been in the IT industry for a while and have an interesting background. Would you mind sharing a bit about yourself with our audience?

KL: Sure! As you said, I'm a little bit on the old side in terms of experience and I've spent far more than 25 years doing this. The two things I would point out is one, was a global data center practice, where we drove digital transformation for clients using cloud and a lot of disruptive technologies. Prior to that, another large international firm focused on high-end enterprises, but really developing out some of the new and original clouds and some of those early practices and also, a very large minor services practice.

DS: A diverse background, enterprise, manufacturers, ton of perspective, and a lot of experience. Thrilled to have you with us today. Before we jump in, I wanted to talk a little bit about the name of the podcast, because there is actually some meaning there besides the sort of the cheeky play on our company name, Aspire.

Digital Aspirations in the Next Generation of Digital Transformation

DS: Digital Aspirations is really about the next generation of digital transformation. Digital transformation has been around for probably five-plus years now, maybe longer. In the first few years, these types of initiatives were most relevant to, in my opinion, the Fortune 100s. We didn't see it in the small interplay space very much, but that is no longer the case. Businesses of all sizes today are placing more and more demands on IT. We see CIOs now viewing technology as a critical enabler for their business strategy and the core to how their organizations are going to differentiate and deliver more meaningful customer experiences and ultimately drive revenue.

This thinking, in my view, is really pushing CIOs to maximize IT's impact on the business and really align technology initiatives to business outcomes that are going to deliver tangible impact to the organization. In our day jobs at Aspire as a systems integrator, this is a quarter of what we do. We have a team of engineers and thought leaders across all architectures - whether it's collaboration, security or enterprise networks, data center and cloud, who are in this case today and provide expertise to clients along their digital journey.

And really, we focus on partnering with IT organizations to help them realize their digital aspirations. So, it's through this lens that we offer this podcast and the goal is really to bring the subject matter experts like Kevin Leahy, Aspire's Data Center Practice Director, to share their perspectives. Kevin, you've been around for a while. Would you agree that business transformation is real and what are you seeing from your vantage point?

KL: What's interesting here, Doug is if I went back a few years, many clients had thought - "I'm not a digital company." They would say that's the born on the web, the born in the cloud companies and they would all point to a variety of cloud-based businesses. But when confronted with that and when I would be advising clients, I would say, "Well, how are you going to transform your manufacturing line?" And they would talk about IoT data.

When asked "How are you going to get the right skills in house?" they would say, "I need the data on the people and what they're doing and how productive they are." They would talk about the need to understand their clients better, be able to see what they're doing. Then, I would sit back and say, "You just defined yourself as a digital company." So, when you step back— it applies to everyone.

Some are more in the transformation game to compete with the AirBnBs and people like that of the world and others are more just simply trying to be far better at what they are and more importantly, to figure out how they mine all that is valuable—whether it's real estate, whether it's people, whether it's their client; mine these and turn them into better outcomes. The word transformation in digital sometimes offends people, but when you probe at it a little bit, they will all say, "Yeah, that's exactly what I'm doing."

DS: Five years ago, when we talked about digital transformation, it wasn't in the context and the terms that you just framed here. It was like, "What are we talking about? And what are we selling? And how are we going to be relevant in this conversation?" I think today, it's really a progressive point, where it's, "Hey, how can I leverage technology to create a better outcome that's really going to move the needle and help my business grow?" So, it's an exciting time.

IT Priority # 1 – Data Protection Has Moved to the Boardroom

DS: Let's jump right into today's topic, which is Top IT priorities for 2020. The first one - Ransomware is very much a real threat today, you read it in the headlines. If you read Gartner and IDC and some of the other researches out there, they typically have security as one of their top priorities every year, but I think it's fair to say that things have changed a bit. Yes, security is a top priority for 2020 but what do we see as being different?

KL: The reality is, data protection has moved to the boardroom. For decades, I've heard people talk about backup which is interestingly a struggle, a challenge, and it was a cost. Today, people are talking about ransomware and it's based on that backup. Of course. But what's different is if you've been attacked—we see cities in Houston, we see it in New Orleans, we see it all over, cities being shut down, central services being stopped, universities stopping operations.

We see it across the board. So, everyone's under attack. And literally, I saw an article recently where city bond ratings were being affected - whether or not they've been subject to ransomware. So, it is 100% a board-level conversation. Now, everyone's a target and most of our clients—in fact, we were about to go to a client to talk about how we can help them address the risk for ransomware and they were under attack and of course, no one was available to meet with us.

So, everyone's aware of it, but most clients are not prepared for it. First thing to be aware is that you are exposed. Second thing is to understand what you do today probably is insufficient. What probably the biggest challenge is that the best protected data from the client's perspective has always been the data

that's for their most business-critical applications. When you do a disaster recovery model, these would be the applications that you would bring on board first.

Now, it's interesting when you then go at it —the data behind there is usually the data that is most at risk from a ransomware perspective. So, what does that tell you? Where they've had the longest instantiated, literally institutionalized processes to protect data is where they're at most at risk of ransomware. Anything that's more than two to three years old in terms of how the process has run, how they analyze, scan files, et cetera, is out of date.

Today's ransomware folks start at the backup copy. They attack the copy and then, they go after the primary. So, when you go to look for your backup copy when you realize you're under attack, it's too late. I also think that it's absolutely critical to understand, if the process is different, best practices are different. You need air gaps, right? You need to check files before you back them up. You need to check them before you restore them. You need to be able to look and compare it to the latest information about what do the actors look like, what do the threats look like. You need to think about new recovery models.

All of these things are different, yet everyone knows they're under attack or at risk being attacked. The good news is there's lots of new tools and things you can automate in that process, in terms of recognizing a threat, of seeing behavior that's abnormal to be able to quarantine that activity and get it off the grids quickly so that it doesn't spread, and knowing ways to build recovery models into the cloud. It's doable, but it's interesting to note that where you're most comfortable in the past, three years ago, you said, "I understand this data, I've got it covered", it's probably where you are at the highest risk now.

DS: What you just described is hugely important, but from a Layman's perspective or a semi-Layman's perspective, it sounds complicated. It sounds scary. As you mentioned, there are some tools out there that can simplify and automate the process, but where can someone start? What are the first building blocks to getting yourself in a better position to protect that critical data?

KL: The first thing is to figure out is, what that data is. You have got to be able to categorize it and decide which data is going to be subject to an attack. So, if you're a hospital, obviously, it's patient information. They will access those records. If you're in a university, then these are certain sets of students' information. It could also be essential services in terms of safety - where police cars are going to be at a given time or similar data like that.

Once you identify that, then you need to look at, what process do I have? And what is the threat? How's it going to be? And how am I scanning those things? First, categorize that data and prioritize it. In most cases, it's only between 10 to 20% of your data that is likely going to be a subject to a ransomware attack. So, that's good to know. Now, you have to figure out how to create some sort of immunity? Do I create another copy? What tools will I use to do that?

Obviously, we work with a variety of partners to be able to help clients identify the data needing protection and the threat itself and to create new restore models. Then, it's the change of processes, to be able to automate it out. It is not sufficient in the ransomware world to wait a day or two and see what happens. By then, you could have crippled the entire business. It's to recognize the threat and again, the tools do that. They provide you with alerts. From here, you need, either in your own processes or through folks like ourselves, to be able to see that event and act quickly.

You don't want a bunch of false positives, but you certainly want to be able to recognize, this is valid, let's quarantine this off, let's take an action. And then, move from there. So, I'd say it's probably those three reasonably easy steps, if you do it. However, they are disruptive, no doubt, because I can almost promise you, like I said, if your existing processes is more than two to three years old, , you're not doing it in a way that's going to be sufficient for today's ransomware attacks.

DS: Yikes! Now from the boardroom perspective, what's reasonable in terms of, God forbid, you get hit with some sort of ransomware attack, you have the proper architecture, processes and automation in place like what was just described, what does that recovery look like in a scenario where you have yourself buttoned up?

KL: The best I've seen, despite of what the vendors will tell you, is about four hours, which is phenomenal to as opposed to days or even weeks I've seen. But it's not as simple as a vendor would tell you, "Just push this button and poof, you're recovered." That all sounds good, but the reality is there's a lot of data to move around. There's a lot of things to bring back on board. So, setting yourself up for an objective and very importantly, testing it is very important.

If you're in the financial markets, you are required to do accessory recovery testing twice a year. But for good practices, they would be doing it quarterly and some, even monthly. Do you have a plan to test for a ransomware attack? It's just a different type of recovery model, where instead of the server's going down, the data is gone, but that's a different lens around what you need to look at your recovery model, and it's that movement of the data, the gravity of the data that is the time-based factor and then, rebuilding everything around that.

IT Priority #2 – Cloud Deployments Reach Scaling Hurdles

DS: Now let's move to priority number two. Clearly, the trend we see today is around cloud adoption. This is a huge thing. When Cisco talks about Cloud, they talk about cloud expansion versus cloud migration. Their perspective is yes, organizations are moving to the cloud, but not everything is made for the cloud.

They're learning that certain applications are going to perform better or there's business readings, reasons why not to move a certain workload to the cloud or why to move. A recent IDC info brief in 2019 said that 92% of customers they surveyed had both public and private cloud environments installed. So, this notion of multi-cloud and hybrid cloud is really becoming the norm for enterprise organizations. With this trend in mind, what are we seeing and where should IT focus their attention?

KL: There's a couple of things, here - one is relative to that 92%. It's interesting what people will define a private cloud to be, and one needs to be cautious. In some cases, those private clouds are really just very well-managed virtualization environments. So, it really comes down to the dynamics required. Everyone is looking for that cloud experience, because that is what's enabling that digital transformation that we talked about earlier.

Cloud experience is the key and the speed. People are moving to cloud for speed and for user experience and in most cases, they recognize that they were spending more to move to a public cloud than they needed to. Private cloud is the cheaper option if they can get it sufficiently leveraged. If utilization is high, it's always going to be cheaper than public. The public clouds are quite profitable as I think everyone recognizes. The challenge is to move for speed.

When you move for speed, you cut corners. Classically, clients would configure the largest images. They would have them up 24 hours a day. Even if you went back almost a decade, the average developer had VMs up 24 hours a day, 7 days a week for six months at a time. You can quickly imagine that cost is going to be a huge issue. So, once you get it up and running, that's great - if there's only a few of them. Unlike people, who own credit cards, 30% to 40% of your IT is suddenly over-configured, not being turned off when it's not used and you can imagine the cost impact.

So, the number one challenge IT is hitting is cost. "I didn't take into account all of this, I didn't really figure that out. I went for speed." The great news is, that application is running fantastic, people are

using it. They're happy with the experience and they're not going to give it up. But how do I manage that cost component? That's one element. The second is the reality of scaling as it sounds really easy as an example, to build a private cloud.

You can stand one up and depending on which hyper-converged vendor you prefer, they can tell you it will be 22 minutes out of a box, 28 minutes from box production, and whatever number you like. However, when you actually look at it, the reality of that is, it changes your infrastructure. It changes what you need to do for security. It absolutely changes east-west traffic inside your data center just as a public cloud dramatically changes the wind traffic you're using and the patterns there.

The second big scaling factor is the network. How do I keep track of both the cost of the network, but more importantly, manage the performance of it and be able to actually deliver that experience? This, versus having a great private cloud, but the latency to it is so slow and I can't achieve the value out of it or I can't get the response time to my developers, because I didn't have the proper bandwidth to the public cloud? So, the second big gap there, if you will, is the network component.

The third, of course, is the storage component - the data. Where is that data? What's interesting when you start an application is that generally, you focus on user experience. There's not a lot of data in that. In a public cloud, it was great. But as applications mature, they tend to demand more of the corporate data and that data classically might sit back inside the data center.

Now, you're back to that point of, should we have been public or private, how do I get access to the data that further needs to get forward and be part of that solution as that solution or that application matures? Finally, the last point that I would highlight is integration. Many things start in isolation but as you move into it, you will realize there are custom modules to consider. An example of this is a SAP environment. In many cases, you can run SAP in a public cloud, but you find out later that you are dependent on custom modules that perhaps can only run inside your data center. This is one of the points of integration that needs to happen as you start to grow and expand.

*So, these are four classic examples where the scaling hits the bubble, as the success of that cloud-like experience and the digital workloads - it's that cost, it's the network, it's the security, it's the integration challenges and being able to access and expand through that integration into other services that will help enhance that experience.

DS: I'm glad you mentioned security there, too, Kevin because it's a big piece of this. The other thing that comes to mind as well is what you described when you throw in this sort of hybrid multi-cloud

environment. From my perspective, it seems to add a degree of complexity to what IT has to manage on a daily basis. What's the challenge there in terms of managing these environments? And is there automation and other tools that can be added to the mix to make this easier?

KL: Absolutely, Doug! That's an interesting challenge, so we should get into this. You see, many people take on cloud. In many cases, the IT directors find out that the company was using cloud because some business line started it and then, it became their responsibility. So, they would start to manage it in the same way that they manage the traditional assets on premise. The problem is the whole point of cloud was that speed on user experience. The processes didn't keep up.

I remember one very large client I was working with in the past prior to Aspire, said to me, "How come your services don't give me the same level of service that the cloud does?" I showed him the contract and I said, "This is what's required for us to stand up a new server. It's three weeks of manual signatures. We had all the automation installed, but those three weeks of manual signatures, the processes to allow the business to use it, held them up.

Even if you have the automation, having the processes to allow that automation to proceed because they've been tested once, should propagate pre-approved changes, so you can do them quickly across a larger scale.

The other part is defining policies. Policies are complicated. In many cases, if you go inside a client environment and ask who makes the decisions, they would point to someone who is in the back room with his back always leaning against the wall. I don't know why that it but it's true. It always seems that way – and he's the guy who makes the decisions.

He figures out all of these things from looking at all the knobs and levers that he has to pull or the information he gets. What you need to be able to do is make some definitive processes that you can automate. As a service provider, we always have the philosophy, if you see it twice, automate it. Automation doesn't help you for the first time, because somebody has to actually write a process out and then do all those things. But if you see it twice, you want to automate it. You want to able to make those definitions. You want to be able to replicate it.

You want to do it based on informed decisions, events or correlation of information from a variety of sources. But then, you want to be able to automate out the tasks to the extent where it's repeatable. So, you actually automate the decision process. The good news is there are tools that allow you to do that. The tools will actually help you go through the process of figuring out what these events are, the artists

in the correlation and the definition of when to do something, when not to do something, when to turn things on, when not to turn things off.

Great examples in clouds, are, people deleting data - developer specifically. You will find a good lawsuit online, where someone sold lost data, or they automated something and created a new server, but that server was outside of a secure environment and potentially, a GDP or some other privacy or governance rule was violated. So, it all needs to be automated in the context of the policies and rules that have to be informed.

Top IT Priority #3 - Internal IT Management Processes, Holding Back the Pace of Transformation

DS: That sounds like a super topic for a future podcast in itself, Kevin. There's certainly a lot to chew on there. We can go deep, so, stay tuned for that one. But in the interest of time and actually, it's a nice segue into our third priority here and getting back to our earlier discussion around digital transformation where CEOs are doing technologies that enable business strategy. In your earlier comments about processes, slowing down that transformation, my question to you as a segue into this third priority is, is IT ready for this transformation? And can they keep pace with what the business is demanding?

KL: Intellectually, they already tend to keep pace now, Doug. That's two different things. This is nothing to do with some of the motivation of IT. The challenge IT has in the client I was just at last week, is that they're desperately keeping the lights on. Yet, in order to actually be able to do this transformation, a couple things have to happen. A).The lights need to stay on and they may even need to reconfigure the lights faster and faster, but they also have this other thing, the classic DevOps.

What is DevOps? Just bring development and operations together to drive those digital outcomes. So, what they need to be working on is those process definitions, the DevOps integration of policies. Only the people who know the business can do that. So, they need to be doing that. At the same time, in order to be able to have the business respond to those things, they need to be able to automate out the outcomes, they need to be able to build an infrastructure and a set of capabilities with the right level of obstruction.

I know that sounds very technical. But if you fundamentally create your policies at the right level, then you cannot really care too much about which technology is underneath and they need to keep the lights on. Frequently, what we find is clients come to us and say, "I need to work on this business policy where the DevOps side is the business outcome side of it. "No one else can do that, because no one else knows my business like I do, but can you-"

This is what the client was asking for last week, "Can you help me by driving the automation and the best practices around that? Can you help me by defining the tooling I should use to be able to obstruct these things out? Can you actually manage parts of this for me or all of it for me so that I can focus on this piece and my folks can make the transformation over here?" Hybrid has introduced tons of new technologies. And it's not just new technologies, it's new processes.

You used to be able to just monitor your servers, your storage, network, and you are pretty well with your applications. Now, these applications are spanning clouds or spanning WANs, so you actually have to do some application monitoring. All right- you have to do a lot more enforcement. You have to have a much faster backup like what we talked about already. And you need to be able to do it across Amazon, Azure, or your on-premise VMware private clouds. You need to be able to expand your legacy infrastructure. You also need to consider that you have a broad application portfolio with a new app popping up every day.

So, dividing where you need to spend your time, figuring out how to leverage partners to help you with monitoring and the speed of execution while you focus on implementing the business strategy to get to that desired outcome is the balance we hear people saying, "That's where I want to be. I need to be here, but I need your help to be able to ensure my infrastructure can do it", because we're always reinventing or reinvesting as well in that tooling, in that automation, in driving that process evolution.

Here's an example, from one of my former customer dealing - we spent 18 months and millions of dollars building out a managed service. Most clients don't have the 18 months and they don't have the millions of dollars to spend to build that sort of capability. They're looking for someone who can invest in that automation, in that platform-driven outcome across the clouds, so they can focus on the business outcome.

DS: So, what I'm hearing then, Kevin and I think everybody would agree, is most IT shops are stretched thin, right? There isn't an overabundance of resources there. And I don't want this to sound too self-serving, but as they sort of evolve and mature from an IT perspective, we're seeing, and I think you agree, at least, in that small enterprise space where we play, a lot more adoption of a partnership to help them fill in those gaps. Is that fair to say?

KL: Yes, absolutely. I wouldn't say small enterprise. I would say it's large as well, because speed is the priority. I have yet to see an IT department saying they were overstaffed.

*Large enterprises in some cases, have an army of IT folks compared to other market segments; but they also have the same challenges as the small enterprise.

They also are more aggressive. They have more applications to support. So, I see that as universal. In particular, none of these applications were built out for cloud deployment complexities whether large or small, for these processes to go across those environments. They all are in the time pressure to be the first one to get there. If you watch what the analysts say, only a small percentage of clients make it through this transformation and a bunch more suffer because someone got there first.

Suddenly, they're lagging in the market when they used to be the market leader. So, the trade-offs to get to speed are there. The custom applications at the enterprise drive a massive amount of their resources where they need to focus. Again, it's back to - where do you need to focus? If you're writing customized, containerized new architecture applications, even if you have 3,090 folks and a new one client who did, 2,000 of them are working on those new apps.

DS: Agreed, Kevin**.** It's aligning those resources. Again, back to those outcomes and filling in the gaps and the operational aspects of IT there that are not business-impacting, maybe to outsource those to somebody that can help.

Well, I appreciate your insights, Kevin. If I can recap, it sounds like the three that we spoke today, of the leading IT priorities for 2020 that you see from your perspective being the data center and the cloud, first being data protection has moved to the boardroom, cloud scaling and integration challenges in the early workload decisions for cloud deployments and then, the third piece is internal IT management processes and making sure that IT isn't holding back the pace of transformation. So, any closing thoughts before we say goodbye?

KL: I think just the point I would reiterate Doug, is, you can read the market studies, the point is that - these are the things we actually see our clients asking us for. And so, I would encourage every one of our clients to recognize, this is not hypothetical as both your competitors, your partners, your peers are making these investments. It’s important to get a good level set of where the market is in order to make sure you're doing the right things for your business.

DS: That's great. Well, I thank you, Kevin, for sharing your perspectives and your insights. And I thank, also, our listeners for joining us today. Be sure to tune in to part two of the top IT priorities for 2020 when our guest will be John Cope, Aspire’s Regional Solutions Strategy Director.

Thank you for listening and we'll see you next time on Digital Aspirations. I'm your host, Doug Stevens. Bye for now.

Outro: 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.

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.