

November 9th

Lexington IT.

Tomorrow we celebrate the 243rd birthday of the United States Marine Corps; to my fellow Marines and friends, Happy Birthday Marines!

This last year I was the CEO of CSRA which we sold to GDIT in April. The company was spun out of CSC, merged with SRA, did an IPO and acquired NES and Praxis before the sale to GD...quite the mouthful and a busy two years.

Throughout this process, Enterprise IT was center stage, both for the markets we served and the company we created and I think provides an interesting case study.

During this process, I learned to listen well to my CIO, John Dancy, and my CTO, Yogesh Khanna. Any good idea or thought that I share today are there's. Anything you think stupid, I will own;-)

We began by creating an IT environment from scratch...with a bias to move everything to the Amazon Cloud but also committed to our deep bench of technology partners across the stack. We recognized that cyber defense needed to be our first thought in designing our architecture and working with our partners...and we also understood how important the transport layer and network fabric would be in this choice to move to the cloud, both for the initial move but also for ongoing operations.

In our initial moves we found the workloads were not moving gracefully and John's team switched to moving data with "big damn hard drives"...and we've now seen the market make good use of Amazon's Snowball and Snow Mobile. But it also made us think about longer term ongoing operations where distance and time might matter and affect the quality of the work.

We recognized that certain work loads would not be moved, for a variety of reasons, and we learned a lot along the way. The reality was we created a hybrid IT multi-cloud environment...with

about 50% of our work in AWS and about 75% in total in the cloud with the rest in our own data centers with thoughts towards an on premise hyper-converged stack.

Hybrid is both private plus public (often with the same vendor), and/or multivendor. IMHO, both forms of hybrid will survive. Government customers will operate hybrid environments, both on premise and off premise and with a mix of legacy and next gen tech, for years to come, and they will do so for good business and mission reasons.

Each government enterprise has literally thousands of app's, many which need to be retired, many replaced and most moved to the cloud. Enterprises also have sources of data, both essential to their applications...as well as data spilling on the floor and not yet mined for value, which is a great first place to accelerate cloud adoption (“shallow end of the pool”).

At CSRA we mapped every VM and moved significant work to AWS. But we also relied on the

future promise and investment in the cloud by Microsoft 365/Azure for so much of our collaborative work, alongside our CRM tool of choice, Salesforce...and it was great to see both partners double down on their commitment to our government customer; within the company, we managed our personnel with Workday; our teams created private cloud mission focused stacks for customers around Red Hat Open Stack/Open Shift or VMware; and we relied on SAP/Hana and Oracle Financial DB for so many of our customers.

Just think for a moment...cutting 6 million transactions a night, where if you miss one, it is a long nightmare until resolved...it makes you double down on the resiliency of a private dedicated offering, for example, using Oracle Exadata running Oracle DB on premise...and someday, yes someday, you might consider Exadata in a public dedicated segment of an Oracle cloud, but you'd honestly think twice before deploying it to AWS, even as you move every VM to the Amazon Cloud.

My point is that the work across the enterprise demands you to broaden your architecture to allow these best of breed companies to help you improve performance and mission.

There are a handful of these ecosystems now emerging, and yes, lately it seems like they are at war. In this enterprise environment you have to create an architecture where CIO's navigate the respective swim lanes of ecosystems led by AWS, Microsoft, Oracle, Red Hat/IBM and Google for ease of integration, but all the while focused on keeping your users happy and improving their user experience (U/X).

These Hybrid environments and new delivery models will require enhanced capabilities/ solutions, talent, and management acumen to address higher complexity as we deal with both the realities of IT today and technologies on our horizon.

Cloud-first is the defacto strategy.

Cyber requires continued focus, visibility and integration into every facet of operations, is critical and must be in the DNA of everything we do and build. Fusion of AI and the Cyber domain for faster detection of incidents and auto-remediation at machine speed will be the norm and our government cyber professionals will need the freedom to actively defend the network, protect their data and gain advantage inside the control plane of any cloud instance, private or public.

AI has the potential to automate every layer of the tech stack. We will save time and labor costs on a myriad of tasks and we will apply AI to more challenging predictive outcomes. Companies that I really admire are going deeper with AWS SageMaker, but many of them are not ignoring competing capabilities from Microsoft, Google, and IBM. In an Enterprise you have to look at multiple options: for example with AI and ML; a Microsoft shop is likely to go with Workbench from MS, for developing ML algorithms; while the rest of the enterprise is deep into SageMaker.

Data is the new currency...actually my favorite Cloudera T-shirt is “data is the new bacon”! We are seeing a full spectrum of capabilities being created to collect, store, manage, analyze, distribute, and apply data for better outcomes.

There are several “Horizon technologies” that must be on everyone’s radar and most of which will drive breathtaking demands on our transport layer and switching fabric. As we served our customers at CSRA, we benefitted from our strategic partnership with Cisco in thinking about how to scale and secure future multi-cloud architectures as they optimize future growth in data and processing power.

5G is being tested now, globally; it will increase bandwidth to end devices by orders of magnitude. The IOT space continues to mature. It will dramatically reduce the time gap between intelligent data, and that data’s impact on outcomes and with IPV 6, data is named and worked at a granular, molecular, atomic level. This will have a transformational impact on what

is extended to the edge and how we use end devices with truly spectacular compute.

Back at the core of the enterprise, Quantum computing brings unprecedented compute speeds that creates new opportunities, and threats; for example, allowing nation state actors to break codes on currently-encrypted systems and applications.

Blockchain is creating buzz in government and viable use cases are emerging that can benefit from this.

We also need to look beyond this horizon which leads me to one, last thought...

...the US is in danger of losing the innovation war to China, especially in AI and ML. The investments by China in next gen technologies, and how they are applied, dwarf what we are doing here in the U.S. It is centrally led by their government with a strategic, long term focus. We are not doing enough in the U.S. We need to support the Congress and the Executive branch,

especially the Defense Department, as they focus our Nation's rich talent of technical ecosystems and their current and future workforce to win this strategic competition.

Thank you,  
lp3