Contain Costs & Increase Predictability:

The Benefits of Cloud for Government

Introduction

It's a staggering number even for the US federal government. Since 2002, and against the backdrop of a budget deficit that's now more than $17 trillion[1], the government has spent $600 *billion* on information technology alone. By any measure of fiscal responsibility, efficiency and accountably, spending on IT during the period can be considered excessive. Yet it's only in the last few years that the spending's root causes have come under closer scrutiny. The overriding reason, of course, is budget control and pressure from the tax-paying masses. But an equally significant reason is the government's approach to technology itself. To put it carefully, certain technology decisions at the federal level since 2002 have been both curious and questionable. A notable example is this:

At the peak of its $600 billion IT spending spree, the federal government built, operated, and maintained 1,100 data centers for various agency and constituent functions.[2] Yet by the government's own admissions, they developed data centers that were much larger capacity than needed — and that were "antiquated" by the time of launch. Since then, these centers have remained immensely problematic to modify and sustain. They are often duplicitous, are cross agency inoperable, and continually fail to deliver on their intended mission. Worse is that a large portion of the government's current $80 billion annual IT budget[3] is spent maintaining this aging infrastructure. (Ironically, current maintenance expenses nearly exceed what it would cost to build the same infrastructure "new" using today's available technologies.)

The cloud as a feasible solution option

Especially as budget reduction pressures mount, it's clear the federal government must change its philosophies toward IT and an infrastructure that's outdated and costly. Getting lean has become mandatory. Moreover with a constituency demanding greater technology ease of use and privacy protection, CIOs and decision makers at the federal level must weigh new technology options and their feasibility. The cloud gives the government one such option, and the present administration agrees.

Citing the administration's Federal Data Center Consolidation Initiative (FDCCI) and its goal for the government to be data center free by 2018[4], the cloud has become integral. Already, a number of cloud initiatives have been mandated in various federal agencies, and the resulting cloud solutions are

[1] http://www.usdebtclock.org.
[2] VanRoekel, Steve, Federal CIO, keynote remarks as prepared for delivery, PARC 2012, pg 3.
[3] http://itdashboard.gov.
[4] Ibid.

showing measurable value by way of cost reductions and broader functionality. However, there's still work to be done.

To truly change governmental thinking toward technology and reducing costs for IT, federal operations as a whole must ultimately buy in to the cloud and what it provides.

Given the magnitude of this outlook, a baseline is that the federal government's current mission objectives for IT mirror those of commercial organizations that have implemented cloud solutions successfully. These organizations report the cloud's prominent advantages to be lower initial capital investment and operational costs, fewer demands on IT personnel, and greater scalability and flexibility. In particular, government contact centers stand to benefit by replacing outdated legacy communications infrastructures with more adaptable and cost-reducing cloud technologies and functionality for customer service. Where government needs differ from the private sector is in the federal level's stricter regulatory, statutory, and policy requirements for personal data security and privacy. The cloud provides the kinds of security controls needed to meet these requirements.

Moving forward, several factors will drive the federal government's decision-making processes for IT. Among solutions they should consider mightily are those offered via the cloud.

The New Government Driver — Do More With Less

The federal government's take on technology and IT spending has already changed decidedly in recent years, and continues to. For the most part, federal IT chiefs now view technology investments the same way many private sector organizations do. That is: implement functionally advanced solutions that cut capital outlays upfront and operations and maintenance costs over time — then constantly aim for the highest possible return on investment. Government CIOs also point to other factors in the technology selection processes. On the list, faster deployment and speed of implementation, scalability, reliability, and more agile on-demand licensing for employees and users. Updating government contact centers for constituent and consumer services is a further need, the core objective being to replace outdated multi-system infrastructures and unify interaction capabilities inherently.

Physical facilities and efficiency are additionally central to new federal-level technology decision processes. To that degree, the government has taken hundreds of wasteful and ineffective data centers off-line, having reduced its 1,100 centers to 472 at the end of 2013. With the initiative to phase out all data centers completely by 2018[5], the objective until then is to reduce energy use as much as possible in each data center still in operation.

At the same time in a related plan to move from legacy systems to commodity IT, the current administration has mandated a "Shared First" or "Cloud First" policy for new technology implementations. Federal Chief Information Officer Steve VanRoekel explained the mandate this way in his presentation at PARC 2012.

[5] VanRoekel, keynote remarks, PARC 2012

> *Cloud moves us away from a capital-intensive model and toward a more flexible operational model where agencies have to pay only for what they use. Shifting to the cloud doesn't just save us money — it often provides better service, including the ability to scale up rapidly in real-time to meet demand.*

It should be noted that VanRoekel has a credible track record. After 15 years at Microsoft and before he was appointed Federal CIO, he initiated the effort to modernize the FCC's IT infrastructure as Managing Director of that agency.

Early signs to look to the cloud

The need for the cloud was never more evident than when the current administration launched its Car Allowance and Rebate System (CARS), more commonly known as Cash for Clunkers. When the system experienced unexpectedly high peak loads out of the gate, the CARS initiative faced unwelcome issues immediately. One cause of the system's early malfunction was a customized commercial application hosted in a traditional data center environment, a combination that failed to perform processing functions at needed levels. But the bigger problem, unfortunately, was that government's premises-based IT model and data center functionality couldn't be scaled fast enough to keep up with demand. Within three days of going live, the CARS system was overwhelmed and suffered several unplanned outages and service disruptions. With no ability to scale quickly, it took more than a month to steady the system and begin processing car registrations to participating dealerships as intended.

Had the cloud been in play for the CARS program, IT chiefs would have been able to avert system overloads by purchasing additional services capacity on-demand. Lesson learned. Decision makers at the federal level are now more focused on preparing for the immediate future as well as long-term, and recognize the cloud's flexibility and potential value. Also in light of IT production issues and consumer problems like those with the CARS system roll-out, it's no wonder the administration established its "Cloud First" policy for IT operations at the end of 2010.[6]

Under the 25-point Cloud First policy, among other mandates, federal agencies were given deadlines to consolidate data centers, collaborate with thought leaders in the private sector, and shorten the procurement process. Noteworthy for cloud providers, federal agencies were required to "default to cloud-based solutions whenever a secure, reliable, cost-effective cloud option exists." At the time the Cloud First policy was announced more than four years ago, the goal of implementing cloud solutions was an estimated savings of $3-5 billion annually.[7] Those estimated annual savings are likely higher now, and will continue to be as cloud solutions become more prevalent in federal agencies.

More recently, CaaS applicability facing the Patient Protection and Affordable Care Act ("ACA"), cloud functionality, agility and efficacy is of utmost import. ACA user uncertainty and inability to register on-line has stretched government ACA related contact centers to the breaking point. The need for CaaS and its licensing and fleet footed flexibility is key in overcoming the logistical customer facing hurdles that permeate this initiative.

[6] Kundra, Vivek, Federal CIO, *25 Point Implementation Plan to Reform Federal Information Technology,* December 9, 2010.
[7] Ibid.

For larger initiatives like Healthcare.gov, the architecture must be agile as well – both the software architecture as well as the broader Enterprise Architecture. However, the principles for Agile Architecture are only now being fleshed out, as ZapThink explains in Jason Bloomberg's book, The Agile Architecture Revolution. As the word revolution would indicate, no band-aid fix will magically turn big-bang software fiascos into lightweight, Agile, customer-focused initiatives. Instead, we must entirely rethink how we go about software delivery to meet the IT challenges of the 21st century. There is simply no excuse for high risk waterfall initiatives any more, at the federal government or anywhere else.[8]

As people grasp the significance and impact of this legislation, CaaS is a key player. Inbound traffic will swing wildly but is in a definite upward grade and the richness and agility of CaaS, as a solution, cannot be ignored.

The Healthcare.gov website's issues resulted largely from a lack of coordination between the site's contracted developers, testing that was woefully inadequate, and other problems with back-end integration. Unexpectedly high volumes at launch were also a problem, although the problem was mostly corrected as required fixes were made to the site's underlying framework. Nevertheless, a cloud environment might well have aided integration efforts and provided broader and more immediate testing and development versatility, although the site's testing issues were due to an inadequate timeframe of only two weeks, not necessarily the testing environment itself.)

The Benefits of Cloud Communications in Government

At this stage of the federal government's initiatives to move to cloud communications solutions, contact centers are a primary aim. But federal IT chiefs have also shifted their view of cloud communications toward enterprise unified communications and business process automation. For government agencies, cloud solutions provide needed flexibility and a broader range of functionally in each of these areas. Just as inviting, cloud services can be deployed on-demand, without sacrificing security and reliability. To constituents, reliable communications, privacy, and the security of personal data rate highest among their ongoing concerns.

Here is a breakdown of the cloud's key advantages as they apply to the federal government in particular. We'll start with the favorable economics of cloud solutions first.

Unified Communications

As the demand on government grows, efficiency at the agent level is tantamount. Unified Communications increases speed to result and responsiveness by allowing the user to use their desired media channel. The drive towards less user effort and improved contact center metrics will certainly be a win-win. The high level picture will reflect a more satisfied constituent and greater agency budgetary results.

[8] http://www.cloudcomputing-news.net/blog-hub/2013/nov/01/key-lessons-of-the-healthcaregov-fiasco/

Business Automation

Business automation is a key component of processes both public and private. The efficacy of it is of extreme value. The value-add it brings to market is the obvious streamlining of operations, reducing the efforts of the agent thus reducing handle times. Furthermore, business automation allow for greater training and internal monitoring opportunities to further improve the call flow and process apparatus.

Lower initial capital investment and operating costs

Cloud communications offer IT solutions that require a low initial investment and provide a pay-as-you-go approach. Any additional investment is on an as-needed basis. In the government's case, these and other factors work together to lower a cloud solution's total cost of ownership during the time the solution is in use.

- **Reduce OpEx and CapEx.** When a cloud solution is implemented, the cloud service provider is responsible for managing and running the services being used. The provider thus bears a large share of the cost of doing business, allowing government agencies to reduce OpEx and CapEx, and reinvest the savings in their own operations.
- **Reduce spending on underutilized infrastructure.** The federal government has already cut IT spending significantly by shutting down aging and underperforming data centers and optimizing communications and other business missions via the cloud. As this move to the cloud continues, spending reductions could eventually total billions of dollars.
- **Access to testing and development environments.** The cloud affords government IT teams a versatile environment both for development and testing prior to releasing any new initiative into production. Teams accrue savings though faster timeframes for development, testing, and implementation, with fewer required resources.
- **Reduce the federal IT energy footprint.** When compared to the current high power usage in government data centers, cloud communications help reduce the federal IT energy footprint via a cloud provider. Additionally in line with various new Power Usage Initiatives (PUI, or "green" initiatives) for administrative processes, cloud technology enables the use of data in a more efficient, green manner.

Improved contact center infrastructure

Government contact centers are literally stuck in the '80s and '90s with the wired PBX systems they still use. Because PBX equipment from this time period was never engineered for IP networks and voice over IP (VoIP), centers are unable to move to cloud-based VoIP without expensive customized integrations. More considerable is the fact that these PBXs are end-of-life, meaning change is inevitable.

Beyond just outmoded PBXs, however, government contact centers must evaluate their existing premises-based communication structures in their entirety. As is common in these legacy configurations, voice, email, web chat, and any other interaction channels stem from different systems.

Separate vendors contribute to the infrastructure, but rarely coordinate system functions effectively since there's little or no capacity for integration. The results of such multi-system frameworks therefore are typically two-fold. Communications channels are segmented and inefficient, as are service processes. And operational, administration, and support costs are much higher because various and unique IT skill sets are required to support each system. Of greater concern perhaps, the system components for known (and ongoing) legacy upgrades are becoming obsolete.

Government red tape and lengthy cycles for budgeting and procurement are creating further headaches for contact center CIOs. Even when required components and vendor services are readily available for on-premises system upgrades, obtaining the needed funding and resources can take several months or years. Realistically, then, the timeframes to complete upgrade projects can be much longer.

"Big pool" effect to increase agent utilization

In the same way multi-system infrastructures segment communications and service processes, they force contact centers to segregate the agent workforce to support calls, emails, chat, and other emerging interaction channels. However, because many cloud solutions for the contact center provide integrated multichannel capability to handle all channels uniformly, agent segregation goes away — at least by technology means. No matter which channel, a contact center can route all types of media the same way, to any agent who's available. Multichannel functionality has made this a common contact center industry practice known as the "big pool" effect. Of course, agents must still be trained and skilled across channels and media types, since responding to customer emails and chats is much different than interacting on a voice call. Nevertheless, by creating a pool of agents, including remote and at-home agents, a contact center reduces overhead by increasing agent utilization. Moreover, service levels for all contact types improve with higher agent availability and faster interaction times for customers.

Government contact centers would assuredly benefit from cloud-based multichannel functionality to maximize agent utilization. (Until recently, government contact center decision-makers rarely considered multichannel functionality as being feasible to acquire and deploy.) With cloud solutions to enable multichannel capability, centers could cost-effectively route calls, emails, chats, SMS — any interaction type — to the same agent group. Further, most cloud solutions now offer consolidated historical and real-time reporting that allows contact centers to measure and manage agent utilization with a consistently high degree of accuracy.

Greater reliability

Cloud communications providers routinely enter into Service Level Agreements (SLAs) with their customers and, if SLAs are violated, can incur substantial penalties or be forced to make substantial concessions. To ensure that SLAs are indeed met, many cloud providers build extensive redundancy into their infrastructure and their processes. With the geographic redundancy inherent to cloud communications in particular, providers are able to offer an SLA of 99.999% application uptime consistently and with the utmost confidence. In a government contact center or agency environment where CIOs demand a solid continuity of service strategy, this high level of redundancy and disaster recovery capability is absolutely vital. It affords a large measure of comfort to any federal organization even during upgrades and disasters.

For system maintenance in contact centers using a cloud solution, maintenance is transparent, and is performed regularly with little or no impact to contact center operations. System upgrades are normally completed on a coordinated basis between the cloud services provider and the contact center. This way, as new features and functionality become available, the provider and customer determine when (and if) an upgrade will be performed and how agent training will be conducted. When upgrades are performed, because communication channels are unified and other key contact center software such as WFO tools are fully integrated, concerns regarding "other" systems being impacted are diminished. In many cases, in fact, such concerns non-existent since functionality is all-in-one and tightly integrated on a single cloud-based platform. (The Communications as a Service cloud offerings from Interactive Intelligence are an example of this approach. The company's *CaaS Contact Center*™ cloud communications solution provides a broad set of applications developed in-house to work together, on one platform, in a tightly integrated fashion.)

Increased flexibility and scalability

In the government space, contact centers with fluctuations in workforce management issues no longer must scramble to ensure agent availability at all times. By design, most cloud communications solutions are developed on a flexible licensing structure offered by the cloud services provider. To meet monthly or seasonal call and interaction fluctuations, government contact centers can maintain appropriate staffing levels (without overstaffing or understaffing) by increasing and decreasing agent licensing on-demand. Centers can also many times activate new cloud-based interaction functionality, such as real-time speech analytics and customer feedback surveys, using a similar on-demand licensing approach. Whether agent counts or new service capabilities, the contact center pays only for what they use.

Unified communications

How would UC benefit federal agencies? BPA could be referenced in this discussion, since it's not prominently mentioned previous to this section or in the Conclusions. [TB]

Faster deployment time

Across the federal government board, interdepartmental connectivity is vital. The near instantaneous ability to provision, manage, and modify solutions is a mission critical benefit of cloud communications. More importantly, cloud solutions eliminate long procurement and certification processes by eliminating the need for hardware, various system components, and facility infrastructure as a whole.

Regulations and Legal

CIOs in the federal government must address, and satisfy, several key concerns before a communications solution is ever implemented, let alone a cloud solution. And warranted or not, a top concern remains the cloud's security. Among CIOs, a serious issue is privacy in a cloud environment, and the legal and political fallout that accompany an accidental (or intentional) release or mismanagement of personal data. More than any other aspect, security and privacy are of paramount importance to agencies and contact center operations at every level of the federal government. The same can be said

for constituents — privacy is a huge and constant concern. Therefore, it cannot be understated that a cloud solution must be private, and allow for complete control in selecting who has access to data within that environment.

Where a cloud solution is concerned, a cloud provider *must* comply with the legal, statutory, and administrative regulations and relevant provisions of the federal government. There is no "wiggle room." In a very abbreviated manner, the following major codes are relevant to any cloud provider.

Security vulnerabilities naturally are a fundamental concern, and are arguably the area of greatest pushback by government agencies to the cloud. Data both in rest and in motion must be protected. The safeguards for data protection are stringent. Agency certification and approval does take some time. All cloud providers must comply with the provisions of the Federal Information Security Management Act (FISMA) to determine security controls. The agency will take into consideration what type of data will placed in the cloud and, if the controls are deemed satisfactory, the agency may grant an authority to operate (ATO).

Once an ATO Is granted, a provider must undergo continuous monitoring pursuant to the specific security requirements, to retain the ATO.

In December of 2011, the Federal Chief Information Officer implemented the Federal Risk and Authorization Management Program (FedRAMP). The Chief Acquisition Officers Council described FedRAMP as:

> *[Providing] Federal agencies with a unified way maintain to secure cloud computing services through the use of a standardized baseline set of security controls for authorizing cloud systems. This standard approach to securing cloud computing systems works in concert with the elements detailed in this paper to create a solid foundation of transparent standards and processes the government should use when buying cloud computing systems.*

While this section addresses only major statutes relating to cloud communications, a few others to consider are: the various NIST provisions, Privacy Act of 1974, E-discovery legislation, and Freedom of Information Act.

Government IT strategy on cloud technology will revolve around using commercial cloud technologies where feasible, launching (and in all likelihood used in conjunction with) private government clouds, and utilizing regional clouds with state and local governments where appropriate. As stewards within the federal government, it is the government's duty to monitor, in real time, sensitive data to ensure it is not released and is stored in a very secure manner.

Conclusion

To successfully implement cloud communications in the federal government space, a provider must meet and overcome the following criteria:

1. Navigate the procurement process
2. Solution must meet agency mission goals
3. Solution must demonstrate a "complete" ROI
4. Solution must achieve agency required SLAs
5. The solution must meet and continue to meet statutory, regulatory, and legal policy requirements

The value-add that cloud communications bring is:

1. Reduced cost of ownership
2. Ease of staying current with technology
3. Reduced OpEx and CapEx
4. Agility and rapid needs-based functionality and scalability
5. Unified communications
6. Dependability — 99.999% application uptime — system maintenance is transparent
7. Interdepartmental operability
8. Service Level Agreements
9. Addresses government "green" initiatives

Amidst an environment of surging budgetary deficits, the federal government has entered into the age of actual budgetary sequestration and enforced debt ceilings. Getting lean is not only en vogue — it's mandatory. Fiscal responsibility, efficiency and accountably is popular with the masses and senior leadership alike.

Out of necessity, the backbreaking fiscal cost of maintaining aged legacy systems will not be sustained. With the administration and the public demanding efficiency, legacy infrastructure is quickly becoming a thing of the past. A 2012 Frost and Sullivan survey indicated that for total governmental short-term cloud solutions, telephony accounts only 6% of cloud implementations. That certainly changes with the budgetary and IT pressures being applied to government contact centers.

More and more government agencies have come to see the undeniable value of cloud communications. In light of this sea-change governmental approach regarding cloud implementations, a tremendous opportunity exists for contact center and unified communications vendors to grow their governmental market share.

While undoubtedly there still exists some hesitancy to adopt the cloud, the benefits of cloud communications overwhelmingly outweigh the fears of those clinging to the edifices of the past.