Streamlining Security

Cloud Adoption in the Department of Defense

In an age defined by technological innovation, organizations are racing to implement the most cutting-edge tools — and their attention is increasingly turning toward cloud computing. Already a firmly-established feature in the private sector, the cloud is also making its way into government: the White House's February 2011 "Cloud First" policy[1] outlined a bold new direction for government IT reform, and in the years since, federal agencies have rapidly warmed to the idea of cloud technologies as a critical enabler of enhanced database storage and computing capabilities. A September 2017 Government Business Council (GBC) survey[2] of government and industry leaders confirms this trend: a plurality of respondents report that their organization currently leverages or plans on leveraging cloud technologies in the coming year. However, the study also highlights a range of cultural and technical barriers to successful IT modernization — obstacles that must be addressed before organizations can truly harness the cloud's immense potential.

Digital transformation is slowly but surely making its way to the Department of Defense (DoD). The Pentagon has long envisioned a platform where services, commands, and agencies can share information and streamline decision-making to optimize 'point-of-the-spear' operations. While the Joint Information Environment (JIE) is an ongoing effort to give DoD decision-makers a strategic IT framework that addresses warfighter needs, the numerous programs operating within JIE's purview continue to yield mixed results. [3]

Faced with diminishing resources, ongoing sequestration shortages, and an increasingly sophisticated threat landscape, military agencies are finding ways to procure solutions more efficiently and expediently than the current bureaucratic environment allows. The rise of 'X-as-a-Service' platforms are helping to make this possible: whether it's Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), or just Software-as-a-Service (SaaS), these service packages enable agencies to treat existing IT pain points at scale with current operational capacity. However, the current DoD environment poses unique challenges to such services, chief among them a cultural aversion to third party solutions and loss-of-control.

These concerns are understandable: charged with safeguarding some of our nation's most classified information, the Pentagon is aware that information leaks of any kind could have disastrous consequences — loss of public trust, exposure of personally identifiable information (PII), and even loss of life at the hands of malicious actors. Due to these concerns,

> Nearly 50% of defense respondents feel that their organization does not adapt quickly to new technologies.
>
> "Making the Leap: Exploring the Push for Cloud Adoption," GBC (2017)

the DoD has long operated on the premise that it must own and provide robust protection for all its assets, including data centers. It's understandable then that the rise of cloud-as-a-service agreements would create some unease, particularly with regard to security: after all, it's not possible for an armed guard to physically stand watch over a provisioned cloud service.

According to GBC's survey, this perception is top-of-mind for many active-duty and civilian DoD professionals:

- 49 percent strongly disagree that their organization adapts quickly to new technologies
- 38 percent are either 'not at all' or 'not very' confident in the ability of their organization's IT infrastructure to adapt or scale to evolving needs

Yet the same survey also finds that security concerns (17 percent), budget constraints (12 percent) and lack of leadership or strategy (12 percent) are considered major obstacles to adoption of cloud technology as well.

Just as striking, 33 percent of respondents say they don't know what their organization's cloud strategy is, while 22 percent say their strategy is still being developed. Meanwhile, half of all respondents were not sure how far their organization had progressed toward cloud adoption, and one-fifth said their organization had given no indication it was planning to migrate to the cloud at all.

Whether it's a lack of familiarity with the benefits of cloud, concerns about the technical challenges it invites, or resistance to organizational change in general, the value that cloud has delivered for today's IT innovations makes it imperative for DoD leaders to recognize – and communicate – the ways cloud adoption can ease such concerns. The military already understands the threat landscape is changing rapidly; the essential next step — understanding that IT is central to an effective threat response — should help its unique culture embrace the potential of cloud.

Charting the Path Ahead

The DoD Office of the Chief Information Officer (OCIO) laid out its vision for the future of the military IT environment in its 2016 "Way Forward to Tomorrow's Strategic Landscape":[4]

Insights from Salesforce

Sponsored Content

According to Kevin Paschuck, Senior Vice President & Chief Operating Officer of Salesforce's Public Sector and Aerospace Industries, many government organizations are running into a "digital dilemma."

"There's a widening gap between where organizations are forced to spend their time — in legacy systems — and where they want to spend their time — in agile cloud solutions," he observes.

This divide, says Paschuck, is becoming increasingly unsustainable. First, there's the enormous cost of managing and attempting to integrate hundreds of applications running on different software and hardware. There's also the complex set of demands DoD faces: with transformational technologies converging with increasingly sophisticated threats, it is crucial that organizations are able to maintain security while unlocking new heights in scalability and effectiveness.

By offloading IT maintenance and operations to the cloud, DoD can focus more of its limited resources on delivering value to citizens and ensuring mission success. However, he cautions, organizations need to carefully consider their selection criteria before embarking on any cloud initiative — and this means choosing platforms that are innovative, open, fast, easy, and trusted. These elements, Paschuck maintains, are essential toward ushering in next-generation service delivery.

Achieving this level of efficiency is critical for the defense community. "Our national security hinges on the DoD's ability to meet and exceed mission objectives," says Paschuck, "and cloud's ability to facilitate easy-to-use, transparent, and frictionless experiences is key toward helping organizations achieve these new heights in innovation."

DoD stands at a decision crossroad facing an information technology future that is fast moving, connected, and highly contested. Innovation continues to accelerate at a rate never-before seen, offering previously unimagined opportunities for the warfighter, coupled with a threat environment that also evolves at speeds previously unconceived. This is the new IT.

[T]he Department's IT must have the same qualities expected from its Warfighters – innovation, collaboration, agility, adaptability, effectiveness, efficiency, and capability in defensive and offensive operations.

In this document, the OCIO sets out eight goals for achieving this vision:

1. Execute JIE capability initiatives
2. Improve partnerships with mission partners and industry
3. Ensure successful mission execution in the face of the cyber threat
4. Provide a DoD cloud computing environment.
5. Optimize the Department's data center infrastructure
6. Exploit the power of trusted information sharing
7. Provide a resilient communications and network infrastructure
8. Improve oversight and execution of DoD IT investments

Central to several of these goals is the Defense Information Systems Agency (DISA), which bears primary responsibility for planning, acquiring and maintaining DoD's compute environment. In January 2017, the agency issued its functional requirements for a Secure Cloud Computing Architecture (SCCA), which includes defining requirements for Cloud Service Offerings that provide Infrastructure-, Platform-, and Software-as-a-Service.[5]

Note the "Secure" in DISA's requirements: According to the GBC/Salesforce survey, 14 percent of respondents see improved cybersecurity and information security as a benefit of cloud technology. The only benefit cited more often than security is the optimization of data management and storage capabilities (18 percent). By comparison, cloud's ability to enhance data sharing and collaboration was identified by 14 percent of respondents.

Compliance Drives Decisions

All federal agencies, whether military and civilian, operate within a complex, regulatory environment that requires certain compliance standards are met. The DoD has its own additional layer of regulatory requirements, further ensuring solutions meet the strictest baseline protocols before advancing to deployment.

Moreover, compliance requires participation on both sides of the acquisition equation. While DoD agencies have to meet the requirements of the Defense Federal Acquisition Regulations System (DFARS), so too must defense contractors -- especially in the sphere of cybersecurity. For example, there is a December 2017 deadline for defense contractors to verify that their subcontractors meet the cybersecurity requirements for any Controlled Unclassified Information (CUI) they share. Cloud service providers already must hold authorizations-to-operate (ATOs) from the Federal Risk and Authorization Management Program (FedRAMP) in order to provide cloud services to military agencies.

The DoD may be slow to adopt new technologies and historically has preferred to design and build its own solutions. However, regulatory pressures and shrinking resources make cloud solutions and 'X-as-a-Service' agreements increasingly more viable and appealing to those seeking the most updated technology. By challenging traditional procurement models and procuring versatile capabilities, the DoD may see its culture grow more receptive and innovation-friendly as time goes on.

Sources

1 Vivek Kundra, "Federal Cloud Computing Strategy." February 8, 2011. https://www.dhs.gov/sites/default/files/publications/digital-strategy/federal-cloud-computing-strategy.pdf

2 GBC, "Making the Leap: Exploring the Push for Cloud Adoption." September 2017. http://www.govexec.com/insights/reports/making-leap-exploring-push-cloud-adoption/141248/

3 Office of the Director, Operational Test and Evaluation, "Joint Information Environment (JIE)." 2016. http://www.dote.osd.mil/pub/reports/FY2016/pdf/dod/2016jie.pdf

4 DoD, "Information Technology Environment: Way Forward to Tomorrow's Strategic Landscape." August 18. 2016. http://dodcio.defense.gov/Portals/0/Documents/JIE/DoD%20IT%20Environment%20Way%20Forward%20-%20DISTRO%20(Aug%202016).pdf

5 DoD, "Secure Cloud Computing Architecture (SCCA) Functional Requirements." January 31, 2017. https://iasecontent.disa.mil/stigs/pdf/SCCA_FRD_v2-9.pdf

About Salesforce

Salesforce transforms the way departments, agencies, and its community of contractors meet the unique demands of today's mission. The FedRAMP-approved Salesforce Government Cloud — the world's #1 enterprise cloud, built for government — gives leadership, management, and employees the mobile, self-service tools they need to connect data, process, citizens, and partners across the mission.

With thousands of customer stories and an ecosystem that includes over 2.5 million developers as well as hundreds of certified partners, Salesforce demonstrates how trusted, agile, proven Cloud applications on a user-friendly development platform deliver better government services and empower modern missions.

About Government Business Council

As Government Executive Media Group's research division, Government Business Council (GBC) is dedicated to advancing the business of government through analysis, insight, and analytical independence. An extension of Government Executive's 40 years of exemplary editorial standards and commitment to the highest ethical values, GBC studies influential decision makers from across government to produce intelligence-based research and analysis.