The Four Pillars of Government IT Modernization

A pragmatic path to successfully embrace digital transformation
Fueled by new technologies and paradigms, digital transformation is changing industries and is enabling organizations to reap unprecedented benefits, including improved efficiencies, happy customers and the ability to expand their reach. But unfortunately, organizations that do not embrace digital transformation are being left behind. They lose their competitive advantage and often cease to exist. Now this transformation is at the government’s doorstep and public sector agencies cannot afford to ignore it.

Digital transformation is the integration of and the modernizing of assets and business processes with digital technologies to deliver sustainable, efficient value to customers, citizens and employees.

The transition requires more than just technical expertise. It is a shift in mindset, organizational culture, leadership and possibly the adoption of different skills.

Modernization requires fundamentally innovating and considering different business models. It is about rethinking how services should be delivered with a constituent-centric view and streamlining processes to be more efficient and taking advantage of the latest in automation. This may force employees to do their jobs differently or it may require a completely different skill set to do their jobs. Modernization also touches all three aspects of a mission objective: people, process and technology.

Any application or business process is made of many interconnected and shared components in the real world. This requires any modernization effort to consider the impact on systems beyond those that are central to the business process. It requires a strategy on how and what technologies to use, their impact on adjacent processes and constituents, a clear roadmap with defined goals.

This paper will examine IT modernization's impact on government, the challenges the public sector faces and a pragmatic way forward in successfully embracing it. We will also specifically examine how the Splunk platform can help public sector organizations embrace this transition.

Modernization in Government

Technology has been a center piece of government operations for decades. The scale of initiatives and constituents each agency serves requires a high degree of automation. Government has also invested heavily in technology to achieve their mission objectives.

But agencies regularly purchased systems that only met their own needs creating silos. This makes it difficult to embrace new paradigms and modernize since these systems often run mission-critical applications or processes. The cost and risk associated with replacing, retraining, management overhead, budget constraints and a fear of reputational damage associated with any prolonged interruptions, has driven agencies to maintain these legacy systems long after official support has expired.

These systems often do not have available upgrades to keep up with technology changes, which creates another silo because the outdated systems do not integrate with newer technologies. This has forced government agencies to spend more than 75 percent of its annual budget in maintaining legacy systems.

Lawmakers saw this structure created a huge technology gap for the public sector, while also increasing its exposure to security threats. This led to the passing of the Modernizing Government Act (MGT) in December 2017.

The act aims to remove any funding gaps that have been slowing down modernization. And combined with the Report to the President on Federal IT Modernization, agency CIOs have the guidance needed to execute on what modernization efforts should be prioritized and the funding to draw from to make it happen.

The report aims to consolidate and modernize agency network architectures by accelerating cloud computing initiatives and promoting consistent security posture across agencies. The primary focus of the act is reducing security risks against government systems. All this while improving efficiencies and reducing costs through shared services ingenuities.
It is important the public sector adapt to processes that can help agencies produce with productivity without compromising efficiencies or quality in order to deliver the pace of innovation the citizenry and mission goals require. DevOps, a software and application development approach in which developers and IT operations teams work in closely throughout the lifecycle of a project, is a preferred method in the public sector and gaining favor in this regard.

As government adds more tools and systems, the volume of data agencies is receiving has also grown. Each new tool creates new data, as well as new storage and computing needs for tech shops. That’s why another key component of modernization is focusing on more efficiently using, sharing, storing and managing data.

This largely means agencies have to revamp the way they manage and upgrade the data centers that house and provide access to all that information. In fact, the Data Center Optimization Initiative (DCOI) requires federal agencies to do just that and it pushes agencies to both consolidate data centers and optimize their operations through better server utilization and automated monitoring of key metrics.

DCOI is a cost savings measure, as well as a call for agencies to think more strategically about how they use resources to achieve goals like cloud migration and shared services.

A Lack of Visibility and Insights Stymies Efforts

Many of the modernization initiatives public sector agencies need to embrace are not new. Cloud-first, DevOps and DCOI initiatives are ones that agencies have been attempting for a while but they haven’t been able to implement due to various issues. A survey conducted in 2017 by the Ponemon Institute, and sponsored by Splunk, of 1,200 public sector IT staff and decision makers pointed to a general lack of confidence when it came to:

- Migrating workloads to the cloud
- Managing data center upgrades
- Handling the scale and complexity of IT operations
- Ensuring efficiency of operations

A lack of visibility and insights into operations is a significant challenge. According to the survey, 62% of respondents said they struggled with managing data center upgrades, 60% with migrating workloads to the cloud, and 60% with ensuring performance and availability of systems to meet SLAs consistently.

Drilling deeper, the survey reveals that some of the primary challenges facing the public sector is siloed systems and operations, the complexity and heterogeneity of systems, a lack of insights into operations, and a lack of resources and skills.

This means agencies lack real-time, end-to-end visibility into systems and operations across an organization, and a lack of expertise and the continued maintenance of legacy systems. Without visibility and insights, IT staff are hard pressed to understand what systems to migrate or optimize, where to transition them to or how to consolidate them. Agencies also struggle to understand any issues if an interruption or disruption were to occur and how to fix them. The challenge is exasperated when it comes to cloud environments, where newer technologies are deployed or when data centers are decades old.

Maximizing the Use of Cloud Computing

The public sector has been given an express directive to maximize its use of cloud computing. Migration initiatives started several years ago with the adoption of a “cloud-first” strategy but the biggest hurdle has been identifying the workloads, conducting the migrations successfully and monitoring them once transitioned to the cloud.

The Public Sector’s Loss of Confidence in Areas of IT Operations

<table>
<thead>
<tr>
<th>Area</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to manage data center upgrades</td>
<td>62%</td>
</tr>
<tr>
<td>Ability to migrate workloads and applications to the cloud</td>
<td>60%</td>
</tr>
<tr>
<td>Efficiency (people and effort) to perform IT operations</td>
<td>60%</td>
</tr>
<tr>
<td>Ability to ensure performance and availability of systems</td>
<td>60%</td>
</tr>
<tr>
<td>Handling the scale and complexity of IT operations you are managing</td>
<td>60%</td>
</tr>
</tbody>
</table>

Source: Ponemon
The Ponemon survey shows that cloud-based operations are making the day-to-day functions of public sector IT staff more complex given the shift it introduces into their larger operations environment. The survey found a lack of visibility into application performance and availability across workloads and an inability to troubleshoot applications are major concerns for the public sector. It is also difficult to understand the system interconnections because agency systems often reside and operate in silos without end-to-end visibility. This makes it challenging to understand what is transpiring across the organization and the assets that are involved in delivering any service.

Additionally, different types of data and applications will require different security measures, as well as varying levels of flexibility and performance. Most agencies will need a variety of cloud solutions to meet their IT modernization needs. And once you start mixing and matching different cloud solutions, like hybrid, public and private, as well as different vendors and difference service models, things start to get complicated. IT administrators need to know how all their cloud solutions are performing and interacting, but it can be difficult to get a clear view of disparate workloads. Without clear visibility, one cloud solution may be unnecessarily scaled to provide significant computing or storage, while another solution goes underused.

**DevOps**

IT modernization may imply tools and technologies to many but it’s just as important for public sector agencies to invest in processes. Modern technology paradigms, and the drive to satisfy constituent expectations in the timeframes they demand, has given rise to agile methodologies, like DevOps.

While a re-engineering process may sound complex, agency IT staff and decision makers feel that DevOps is actually making their work simpler, according to the Ponemon survey. Forty-five percent of respondents mentioned that they see increased funding for DevOps. Agencies are also looking to deliver mission-critical applications through this model.

But implementing DevOps isn’t as simple as getting developers and operations teams to talk more. That’s certainly a good start but because of the technical complexity of software development, both teams need a set of tools that support code-sharing, development, automated testing and collaboration.

The biggest challenge to widespread DevOps adoption is legacy systems. Unfortunately, many development tools haven’t been built or deployed to support the sharing that DevOps requires. This causes teams to struggle with a lack of visibility into each other’s’ tools and systems, as well as the data that lies within them.

To gain the real benefits of DevOps, teams need a single place to access and analyze data. But instead of ripping out and replacing individual tools to give every team member the same technology suite, agencies can install a single platform that brings data together from existing systems.

**Data Center Consolidation Initiative**

The Data Center Consolidation Initiative (DCOI) aims to push agencies to both consolidate data centers and optimize their operation through better server utilization and automated monitoring of key metrics. But it isn’t the first time government has tried to reign in data center sprawl.

The Federal Data Center Consolidation Initiative was established in 2010 to reduce the number of federal data centers. But the effort was daunting for agencies. In fact, the Government Accountability Office found there were more than 11,500 data centers by the end of December 2016. That led to a second attempt to reduce the number by government and the creation of DCOI.
Agencies are required by law to achieve and maintain listed target values covering energy metering, power usage effectiveness, ration of virtual machines to physical servers, server utilization and facility utilization by the end of fiscal year 2018. Agencies will also be required to use automated infrastructure management in lieu of manual collection and reporting of systems, software and hardware inventory.

### Shared Services

Shared services enable agencies to overcome not only constraints in budgets but resource and skills gaps as well. Modernization inherently involves innovation and a lack of training or expertise cannot always be the barrier for adoption. With shared services, agencies or departments pay only for what they use and do not have to invest, manage and maintain individual systems and applications. This frees valuable funds for other initiatives and it also reduces times spent on IT maintenance and management. A common service delivery model also ensures consistency across recipients of shared services, promoting a healthy and uniform cybersecurity posture.

The report on IT Modernization focused on two areas: continuous diagnostics and mitigation (CDM), and security operations centers as a service (SOCaaS). CDM is a Department of Homeland Security initiative to deploy and standardize security and data monitoring tools across the federal government. Security operation centers (SOC) collect, organize, monitor and provide central visibility into the state of security on an agency’s network. A security intelligence platform is central to a SOC’s objectives.

To help facilitate the public sector’s migration to new technologies and embrace shared services, agencies need end-to-end visibility into systems and applications in real time to understand the dependencies and relationships between them. Provider agencies need the ability to monitor usage at a detailed level for shared services to be successful so receiving agencies have the necessary transparency and the central provider can bill recipients appropriately.

### Enter Splunk

The MGT Act and the report on IT modernization provide the necessary roadmap to innovate and transform government agencies. These initiatives are not new but they have not found government-wide adoption primarily because the public sector still lacks insights and the ability to gain end-to-end visibility across silos of operations and heterogeneous systems. Splunk provides visibility and insights into migration and optimization efforts, and the availability and performance of applications and processes. It enables the discovery of powerful insights during and after migrations to overcome challenges, drive successful modernization initiatives, address exceptions, improve efficiencies and deliver superior citizen experiences.

One of Splunk software’s key differentiators is its ability to collect data once and use it across several use cases including security and risk management, compliance, IT consolidation and optimization efforts, citizen services delivery, data center optimization and shared services, and more. This ability to derive value from the same data across disparate initiatives improves the return on investments and efficiencies.

Splunk software helps organizations migrate nearly any workload to the cloud by providing required visibility during planning, development, migration, testing,
and production phases of a cloud migration. Before migrations, Splunk can track performance baselines and service KPIs, assess security, offer discovery of the portfolio, provide workload characteristics for candidate selection and assist with capacity planning. During migrations, Splunk software can track progress and offer in-flight performance metrics, help monitor the service and troubleshoot, track environmental dependencies, offer real-time capacity planning metrics and assess security. After migrations, Splunk helps monitor application, workload availability and performance, or both. The platform can assist with cost management and optimization, assess security, monitor service KPIs and provide visibility into governance and compliance activities.

Public sector organizations can also embrace DevOps with the Splunk platform. Splunk software makes it easy for data to be collected from across the entire development lifecycle, indexed and correlated for analysis. Once the data is in, it can be easily searched and visualized based on the objective. It can provide insights into any environment, including testing, staging and production. And developers can search and visualize data from production environments without having to physically access production machines. Agencies can also gain power insights without custom algorithms or acquiring additional complex software with the ability to log and access information about the way their applications and users interact with systems.

The Splunk platform empowers agencies to track capacity utilization and availability of managed space including floor space, rack space, PDU power capacity, circuit breaker load, cooling capacity, patch panel ports and physical servers. It also helps predict future capacity needs. The platform also tracks energy efficiency information, such as power usage effectiveness (PUE), including any supplementary tools and instruments.

Splunk also provides insights and monitors virtual machines and physical servers, such as OS servers, web servers, app servers, and database servers for utilization, and to calculate and meet the targets of DCOI. Generate any DCOI report in seconds and automate reporting to compliance analysts and auditors with scheduled searches and reports in real time.

Splunk offers a flexible and fast security intelligence platform to power a SOC and make its personnel and processes more effective. All SOC personnel have quick access to all the data and contextual information needed to quickly detect, investigate and respond to threats. Splunk software can also help automate incident response processes and playbooks to decrease time-to-remediate and increase efficiency.

As part of task order awards 2A-2E under Phase 1 of CDM, Splunk will be used at the 25 largest civilian Departments and Agencies (D/As) covering 97 percent of the federal civilian government workforce.

Want to learn more about how Splunk can help your organization embrace IT modernization? Contact a Splunk expert now.