Chapter Ten

Use Technology to Enhance Productivity

By Mark Forman

Use Technology to Enhance Productivity

The Problem

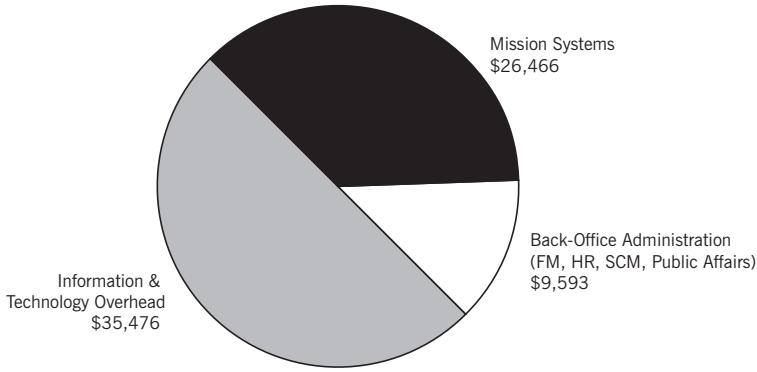
Government today spends more on information technology (IT) overhead costs than on the direct costs of mission systems. This is because government now has thousands of mission systems using legacy architecture, each built for a single purpose to support the needs of a single program or agency. Common standards, common definitions of like data, or enterprise approaches are rarely used in the federal government. Government does not often leverage IT to make things simpler, generate economies of scale, or increase collaboration. Over the last 20 years, mission systems have become more customized and focused on single programs or needs, making government information systems at once more siloed and complex.

An example of the use of legacy architecture and customized systems is the Army's implementation of three different versions of SAP, an IT software system meant to improve back-office operations by integrating business processes. The Army is spending billions of dollars on three different contractors, each independently implementing a portion of the software as if it were not an integrated package. The Government Accountability Office reported that "… representatives from the three systems were not able to articulate (1) what specific data would be exchanged between the three systems and (2) which system would be considered the official system of record for the master data that needed to be consistent between the three systems."[1] To respond to this problem, the Army has created a new IT system and hired a fourth system integrator to connect and reconcile data across the three customized SAP implementations.[2]

Customized mission systems require expensive tools and large specialized staffs to manage complex operations and maintenance activities. The Government Accountability Office reported in October 2011 that $26.5 billion is spent on systems that directly support agencies in the performance of their missions, while $35.5 billion is being spent on overhead costs to manage those systems (see Figure 10.1).[3] The following questions need to be answered in order to get more value out of government IT spending:

- Why does the government spend more on managing IT than on the mission systems themselves?
- How would the government benefit from new technologies, and what specifically should be done to change government's current IT infrastructure?
- What is the role of the chief information officer (CIO) in addressing the cost and use of IT?

Figure 10.1. Spending on Systems Management Exceeds Spending on Systems (Government IT Spending In $B)



Source: U.S. Government Accountability Office. Information Technology: OMB Needs to Improve Its Guidance on IT Investments, GAO-11-826, September 2011.

A New Strategy for Government IT

In today's difficult budget environment, government needs to cut costs and improve results. In addition, today's policy issues require data, analysis, transparency, and program operations that cut across multiple government agencies. Since government's operations are information-intensive, its ability to operate effectively and efficiently depends on how well it uses IT to access and manage information. Government's long-standing approach is to buy and customize systems for individual program needs at each agency. This approach separates information and operations into silos that constrain government's efficiency and effectiveness.

Government needs a new strategic approach to IT. A new strategy would use cloud computing architectures to create less complex, less costly, and more collaborative tools. The new strategy would use new IT tools to improve the timeliness, performance, and cost-effectiveness of government operations. The federal government's current IT reforms focus on reducing IT spending (which accounts for less than 0.01% of federal spending this year). Instead, redirecting current IT spending to focus on improved mission operations of government would be a more beneficial and cost-effective strategy. Specific benefits of a new strategy would include fewer erroneous payments, reduction of risk in loan guarantee programs, quick identification of effective and ineffective programs, and reduced cost of government operations.

Implementing a New IT Strategy for Government

Many argue that government productivity is now directly tied to how effectively it uses IT. Government should take advantage of new approaches for rapid deployment of IT capabilities by acquiring IT as a service; this practice is now commonly referred to as cloud computing. Instead of new capabilities requiring large capital investments and years of sophisticated project management, today's cloud computing services improve agility, cost-effectiveness, responsiveness, openness, and results from government programs. Many cloud computing services are now widely recognized brands, such as Salesforce.com, Google, and ADP Payroll Services.

The 21st-century IT infrastructure is being built around cloud computing, enabling organizations to adopt a new productivity model. Cloud computing incorporates both a continuation of the long-term trend toward automation and commoditization of transactional processes and a newer, rapidly growing trend toward broader access to problem-solving tools. This new productivity model moves people out of rote processes, which can be automated with fewer errors and lower cost, freeing resources for higher value activities. This productivity model recognizes that information is abundant, and that productivity gains can be driven by insights from individuals coming together to share problem-solving ideas and provide the diverse perspectives needed to understand how to trade off costs and benefits of government policies and operating alternatives.

How can government use cloud computing to improve efficiency and effectiveness? A successful strategy would focus on transforming two types of business processes:

- **Transactional government operating processes, including payments, inventory management, commodity purchases, and report filing.** These should be simplified and standardized into repeatable, low-error rate automated tools that take advantage of economies of scale.
- **Government analysis and decision-making processes,** which should be transformed into team-based problem-solving environments that collaborate with government and non-government experts, leverage new data sources, and employ new analytic tools.

Transactional government operating processes. This productivity improvement strategy builds upon long-term trends in automation and commoditization. Back-office operations of government are among the biggest opportunity areas, since they account for $9.6 billion of federal government IT spending and comprise human resources, financial management, supply chain management, procurement, public affairs, and similar systems. Today, these are acquired, customized, and managed as siloed systems, even when the government buys the integrated end-to-end business process software.

Historically, individual agencies have implemented separate systems for each back-office function, with large (sometimes billion-dollar plus) capital

investments including software, hardware, and systems integration services. As a rule, government hires systems integrators that customize proven software, rather than modifying government business practices to adopt the embedded controls and automated business processes. To make these systems work together today, government uses manual labor, either to take data from one system and enter it into another, or to correct errors caused by inconsistent data across multiple systems.

A good example of the potential of cloud computing to assist in back-office operations is in the area of unmatched, or unreconciled, funds. Today, government bears the cost of significant growth in both unmatched funds and staff years devoted to reconciling transactions produced by these systems. As of 2010, the unmatched funds for the federal government totaled $17.4 billion. It is hard to validate the government's calculus of spending about $9 billion per year and generating nearly twice that in accounting errors that cannot be reconciled, as well as the untold staff hours spent reconciling billions more. If government adopts cloud computing services, it will be forced to use standard practices and shared services.

Government analysis and decision-making processes. Cloud computing tools enable more rapid, high-quality problem-solving to improve productivity. Studies show that problem-solving improves when people develop ideas and then use tools to share those ideas in a collaborative environment.[4] As a

Harvesting the Raindrops of Cloud: Moving to the Cloud[5]

By Johnny G. Barnes

It's time to think about Information Technology (IT) as a way to dynamically address organizational challenges and business risks. As the federal chief information officer has noted, moving to the cloud offers U.S. government departments, agencies, and organizations tremendous opportunities to improve mission readiness, expand business and technology capabilities, and reduce the cost of IT infrastructure.

Before moving to the cloud, organizations must answer two critical questions:

- **Location:** Should the virtualized development-test and/or production environments be in an organization's own data center or should the organization buy this as a service from a remotely located cloud service provider?
- **Governance:** How will the organization go about gaining acceptance and buy-in for a shared environment from its leaders and users? How will the organization ensure the agency's IT investment is updated and secure? Government leaders should consider the cloud paradigm as foundational to reducing cost. There are three computing cloud models and a single storage cloud model:[6]

- **Public cloud** is a cloud infrastructure owned by a cloud-services organization and made available to the general public or a large industry group. A public cloud delivers a select set of standardized business processes, applications, and/or infrastructure services on a flexible price-per-use basis. Its strengths include improved standardization, zero footprint on premises, enhanced flexibility, and very rapid service deployment. Most CIOs perceive the weaknesses of a public cloud to be security, privacy, and support.
- **Private cloud** is an infrastructure operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. A private cloud's strengths (vs. the public cloud) include improved customization, efficiency, security, privacy, and centralized control. However, cost optimization is limited to the agency's ability to fully leverage the private cloud services at a high utilization level.
- **Hybrid cloud** is a composition of two or more clouds (private or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application. A hybrid cloud helps optimize critical applications and data use within the private cloud portion while moving peak loads and less critical operations to the public cloud. For example, such an approach could facilitate federal emergency services by allowing rapid public cloud service expansion during an event such as the Haitian earthquake.
- **Storage cloud** is simply the delivery of virtualized storage on demand. A storage cloud provides self-service acquisition and use of storage on demand with common names. Such a facility could serve an agency's dynamic storage requirements as long as federal information security requirements were addressed.

Using definitions provided by the National Institute of Standards and Technology (NIST) is intended to help government leaders compare apples to apples and empower decision-makers with the necessary information to determine which cloud is most appropriate for their organization. The major decision factors influencing cloud adoption by agency CIOs are risk, cost savings, increased IT flexibility and maturity of public and private cloud services, security, privacy, and support.

Government can use private, public, hybrid, or storage clouds effectively for subsets of both its applications and data portfolio, realizing their associated benefits, by considering (1) existing data center investments vs. planned growth and (2) security/privacy/support requirements. At a minimum, government should be able to realize a 25-percent reduction in its operational budget of the application and data transitioned to cloud environments.

Consolidating an agency's IT infrastructure on the cloud can enable government to "do more with less," comply more easily with federal security mandates and initiatives, and most important, meet mission requirements with enhanced capabilities.

Johnny G. Barnes *is IBM General Manager for Technology and Chief Technology Officer.*

result of IT infrastructure changes made to implement the 9-11 Commission findings, there has been significant progress in the area of counterterrorism. Other examples include the Recovery Accountability and Transparency Board's use of transparency concepts and tools. Using these tools, citizens identified potential fraudulent behavior, yielding 7,600 complaints from the public that have led to about 1,650 investigations for fraud, waste, and abuse. Both of these advances resulted from the adoption of cloud computing approaches and tools for collaboration, data sharing, and analytics.

Studies show that using old technologies like e-mail to collaborate often decreases productivity. Such tools were improvements over hard-copy mail, fax machines, and travel to meetings, but are now ineffective tools for rapid sharing of large documents and data. For example, many federal agencies have significantly over-invested in equipment to store and manage terabytes of data that turn out to be multiple copies of the same documents being shared as an e-mail attachment. Newer productivity tools share access to documents and engage members of a group in discussions of issues and solutions. Procter and Gamble provides one of the best known examples of IT infrastructure investments that lead to productivity gains. *CIO Insight* Magazine reported that the cloud initiatives and other innovation have, collectively, enabled P&G to save "'$800 million in costs, [while] innovating three times as much' as it once did, says [P&G CIO] Passerini."[7]

Making It Happen: Recommendations

Government will have to change the way it has traditionally bought and managed IT. It must now move to a service-based construct. Historically, client-server architectures fit the government's traditional desire to buy systems developed or customized for use by a specific program. Such systems required large capital investments and unique project management expertise. Cloud computing confounds traditional government IT capital investment, enterprise architecture, and IT security controls. As an outgrowth of the new strategy, the following will need to change:

- The role and function of the chief information officer
- IT capital investment and spending processes
- IT purchasing processes

Over the past 10 years, technologies (such as virtualization) and IT security and privacy concerns have driven chief information officers (CIOs) toward being the "chief geek" or "control gate" on agencies' use of technology. The CIOs have developed governance systems around a capital planning and investment control (CPIC) process which monitored legacy IT projects to build customized client-server systems. To become operational, the systems had to pass through controlled pre-production and integration testing before being

deployed in the production environment of the corporate data center. These approaches were built before proven cloud computing tools were available as an alternative to client-server architectures. Moreover, they rarely included a means to determine when existing systems were ready for replacement by newer approaches, such as shared services or cloud computing offerings. CIOs will have to become the change agent for modernizing government in the 21st century, and that includes changing their own operations. To implement the new strategy of using cloud computing, we recommend the following.

Recommendation One: CIOs will have to maintain traditional IT controls, while developing new paradigms for managing IT-as-a-service models.

Increased use of cloud e-mail tools is just the tip of the iceberg. Many fear the growing cyber threat environment will be exacerbated by cloud computing. Done correctly, cloud-based solutions offer better security than government data centers, which now contain much redundant data.

Many IT and program executives may be threatened by the loss of control implicit in the increased use of cloud computing. As we look toward the future, cloud computing services will offer government cheaper solutions than similar IT delivered by a government data center due to:

- Improved economies of scale
- Specialist providers with expert, dedicated staff
- Newer, more efficient data centers
- Highly commoditized hardware
- Whole-scale adoption of virtualization
- Aggressive use of open source software
- Higher utilization rates for IT assets
- Competitive market forces

CIOs will need to develop and obtain agency agreement on a hybrid cloud computing vision that provides advantages of ownership (including security and privacy controls), while rapidly obtaining the benefits of new tools and economies of scale.

Recommendation Two: In the immediate future, CIOs will need to identify and prioritize replacement of legacy IT with new cloud-based service models.

The new approach must recognize that government is no longer dependent on its own IT organization, and that the discussion must focus on which cloud computing tools can drive big gains in mission operations productivity. The emerging CIO role will be IT services brokering and sourcing, including overseeing the identification, evaluation, and acquisition of cloud-based services for transactional business processes, data, analytical tools, and collaboration. At the same time, the CIO has to create and maintain robust enterprise information assurance services. The CIO must be both the chief geek and identifier of strategic use of emerging IT solutions.

Mark Forman *was the first Administrator of the Office of E-Government & Information Technology in the Office of Management and Budget. He is currently co-founding a new venture, Government Transaction Services.*

Notes

1. U.S. Government Accountability Office, *DOD Business Transformation: Improved Management Oversight of Business System Modernization Efforts Needed,* October 2010, GAO-11-53, p. 60.

2. The United States Army awarded contract W91QUZ-11-D-0018 on April 15, 2011 for $159,676,827.00.

3. U.S. Government Accountability Office. *Information Technology: OMB Needs to Improve Its Guidance on IT Investments,* GAO-11-826, September 2011.

4. For example, Nicholas W. Kohn and Steven M. Smith, "Collaborative Fixation: Effects of Others' Ideas on Brainstorming," *Applied Cognitive Psychology,* May/June 2011, pages 359–371.

5. IBM Center for The Business of Government: Strategies to Cut Cost and Improve Performance Blog. (http://www.businessofgovernment.org/blogs/cut-costs-and-improve-performance)

6. National Institute of Standards and Technology. (http://www.nist.gov/index.html)

7. Don Reisenger, *Procter and Gamble CIO Shares Outlook for 2011,* www.cioinsight.com, September 4, 2010.