Making the Case for Cloud Computing to Business Leaders

Elizabeth A. McDaniel
National Defense University iCollege
Fort Lesley J. McNair
300 5th Avenue, S.W.
Washington, DC 20319

Abstract- The transformation of government to cloud computing is not an IT implementation. Business leaders must embrace cloud computing and the new information environment as a business strategy for enhanced productivity.

I. INTRODUCTION

Sisyphus the king in Greek mythology, as punishment for some of his deeds, is compelled to roll an immense boulder up a hill, only to watch it roll back down, and to repeat this throughout eternity. Some days the change management challenges associated with the transition to cloud computing can feel like pushing a boulder up hill.

I have been studying cloud computing for the past six months. As a government business leader, and not an expert in information technology, per se, I am fascinated by the challenges associated with the inevitable transformation to this new paradigm. The transformation is even more exciting than it might be in the private sector, because of the culture, bureaucracy, and national security imperatives that must be addressed when the organization or business is government.

The changing roles, responsibilities, and success factors of Chief Information Officers are of interest for me. The most effective CIOs understand and connect to the business, and speak in the language of the business, not IT. Recent Gartner research reports on the potential of cloud computing to transform organizations into next generation digital enterprises. This transformation will require CIOs to engage in "creative destruction" - a process by which they re-imagine the role of IT and their organizations. Creative destruction, or destructive creation, is a process of change in which new resources come from the dismantling and redirecting of existing resources. CIOs must dismantle the current IT hardware, systems, and practices that they built and maintained, to embrace new resources "in ways that redirect and liberate resources to deliver greater innovation and value" [1].

The transformation of government to cloud computing is not an IT implementation, as we have known them in the past. To facilitate the transformation to the new information environment enabled by cloud computing, leaders must leverage and exploit broad sources of power and influence because "there is no such thing as a pure IT project anymore. Whether investments are more IT-intensive or less so, they are all business projects"[1]. Business leaders must embrace cloud computing and the new information environment as a business strategy for enhanced productivity.

What follows are two dialogs between an enthusiastic IT Manager/CIO who is trying to persuade a Business Leader to make the transition to the new information

environment.

DIALOG #1

IT Manager/CIO: Business leader, sir or madam, may I have a few minutes of your time to tell you about this new and exciting approach to information technologies?

Business Leader: I don't have much time to think about information technology. That's your job, and in this climate I have no money to invest in more IT. Those expensive IT systems that came to me for urgent approval were "must-have" projects. The organization spent lots of valuable funds on IT projects that did not meet expectations, and their percentage of our budget just keeps growing. Your job is to keep the back office running smoothly and efficiently, and to stop asking for more money for computer refreshment, expensive ERP upgrades, new staff and system add-ons for security.

IT Manager/CIO: But sir or madam Business Leader, this new cloud computing stuff is way-cool and will provide us new capabilities, features, and benefits once we make the transition. Once we consolidate, virtualize, abstract the services, data centers, applications, secure the hypervisors, minimize the attack surfaces, and yada yada yada…

Business Leader: Thanks but no thanks. It sounds like more IT hype and IT speak. I don't like that we spend millions every year to run our current e-mail, Exchange, Outlook, Sharepoint, EXCEL applications, and servers and data centers. The annual costs includes licenses for users, whether or not they need the complete suite of these tools, to update new software and hardware, employ an army of security staff to insure every computer installs software patches on every machine, and staff to stand up and manage servers for every new system we implement. We are spending much too much money on hardware, software, and staff to keep the infrastructure running, and secure. I am aware of the cyber-security challenges facing us, and know the IT team is focused on the vulnerabilities of each account, application, computer, and server. As a result, our current IT staff is not responsive to users, is challenged to keep up with the security patches and the sophisticated challenges associated with information security. I am not satisfied with our current systems, but I am not confident the current IT staff has the capacity to take us to a new level.

DIALOG #2

IT Manager/CIO: Business leader, sir or madam, may I have a few minutes of your time to tell you about this new and exciting approach to information technologies for our organization?

Business Leader: I don't have much time to think about information technology. That's your job, and in this climate I have no money to invest in those expensive IT systems that came before me as "must-have" projects. Your job is to keep the back office running smoothly and efficiently, and to stop asking for more money for computer refreshment, expensive ERP upgrades, and new staff and system add-ons for security.

IT Manager/CIO: Sir or madam, as the CIO of this organization, I am the chief innovation officer. I want to tell you about a new information paradigm that can improve organizational performance, decision making, information sharing, and collaboration, and save the organization money in the long run. This new paradigm can make all members of the organization

more productive, mobile, effective and efficient, and innovative, and at potentially lower costs.

Business Leader: When you talk about innovation to improve the business and to foster effectiveness and innovation, you have my attention. I believe there are IT systems and tools that have the potential to support innovation, networking, collaboration, and information sharing. And if this new paradigm might save us some money down the road as well, then I am willing to listen.

IT Manager/CIO: Let me paint you a picture of the current information environment. Our organization and individual users rely heavily on information and communications technology to accomplish their missions. We conduct our work using desktop computers from offices, as well as mobile devices, from home as well as locations worldwide. Local organizations purchase these computers and appropriate software licenses for each user (generally through enterprise licensing agreements) to communicate via email, create documents, organize and sort information, and do various levels of analysis, generally using a standard set of desktop applications that require individual licenses.

Information is fragmented because users cannot find what they need in their files, nor can anyone else. No one knows what other users know, and nor can anyone access data when needed. Users save documents, calendars, contacts, and emails on their machines and/or on organizational network drives where they are password-protected and accessible only to themselves. All users suffer with overflowing email in- and out-boxes with attached files containing data that may or may not be of enduring value. We create ad hoc file structures unique to our requirements, and our data is generally not searchable unless specific arrangements are made using organizational network drives where shared folders/files are established. When the keeper of that information moves on, the incumbent typically has no access to relevant information and files, which hampers productivity and continuity and puts the mission at risk. This leads to sub-optimal decisions, under performance, and the potential of organizational failure. When information sharing occurs, it is the result of valiant, individual, and ad hoc processes that are not built into the systems.

In complex government organizations individual components and activities make decisions that define their environments. Although standards exist, actual implementation is left up to the local organization to build its own IT infrastructures with web, email, SharePoint, and other services, and to be responsible for the security of that infrastructure. This fragmented approach reduces opportunities for maximizing utility, limits ability to scale to meet short-term needs, inhibits cross-boundary collaboration, and makes economy of scale nearly impossible. The current model encourages inefficient use of resources, limits visibility of support funding, and drains precious organizational funds from more critical mission requirements.

Despite more pressing priorities, our organizations are spending more on IT than ever before. Most organizations support their own infrastructure, storage, applications, licensing, training, and Help Desk functions. They have their own teams of IT specialists who do provisioning, keeping systems and networks running, and users functioning in a time when operating

systems and desktop applications are more numerous and complex than ever.

The current computing desktop model distributes responsibility for security to individual organizations. Users must sign in many times a day to gain access to multiple programs and applications, an often wasteful and frustrating practice. IT staff at each organization are responsible for the security of their own desktop installations, servers and networks, and for monitoring, protecting and updating them, including patch and vulnerability management. Additionally, IT staff is responsible for addressing all user requirements, with varying levels of knowledge and sophistication of leading-edge security practices. However, in government organizations, as in other large dispersed organizations, these computers and servers are connected internally and externally, exposing vulnerabilities in one organization that may compromise other organizations with which it is connected.

Business Leader: OK, I get your point. You make me realize how accustomed we have become to the constraints of the current environment. Help me imagine a new environment that enhances organizational performance.

IT Manager/CIO: Let me paint you a picture of a new information environment enabled by cloud computing. Users will be able to collaborate, communicate, learn, innovate, lead, and make knowledge-based decisions to facilitate the mission of the organization. They will be more productive and collaborative, and can make better informed decisions, while appropriately and securely sharing information.

Users will have better access to the right data at the right time, and searchable data is available wherever users are. Users and organizations can share, as well as appropriately restrict access to data according to its purpose and audience. Users only need to know how to use their data, and unlike now, do not need to think about where it is physically located, how to archive it, or back it up.

Using inexpensive, agile and light-weight machines, users can access their applications and data easily from any location, regardless of their connectivity. They will no longer need to save documents on CDs or send them as attachments via email for access in other locations, which means that data will no longer get misplaced or stolen. They can pull together data quickly from multiple sources to draw conclusions necessary for performing their missions. The data they produce can easily be made available to others with the proper access and to their successors in their positions. Ultimately, institutional knowledge is made permanent for better, more efficient decision making.

Business Leader: Business Leader: Does the new environment that facilitates this enhanced decision making and information sharing rely on enterprise solutions?

IT Manager/CIO: From the enterprise perspective, this new infrastructure increases utilization of hardware and centralizes administration of many of the most common IT tasks. Organizations are freed from operating on-site storage, servers, applications, software, and security facilities and management, thereby saving real estate, power, and staff costs at every level of organization. IT becomes a service not a capital expense.

Economies of scale allow for a level of security from the uniform enforcement of security measures. Standardized, centrally managed builds of low-level infrastructure

can be more easily and quickly maintained and updated to protect against the latest threats. Movement of application functionality from the desktop to the server environment allows for reduced complexity, opening the door for the use of thin -- or at least thinner-- clients, and thereby reducing the desktop attack surface as well.

Sophisticated security experts can focus their attention on the security of information, as well as software, servers, and systems. Information security can be increased through consistent centralized security administration that fundamentally changes the way software patches are propagated and vulnerability mitigation is accomplished, and identity management leverages a secure, integrated single sign-on solution.

Business Leader: I think I understand. Please list the benefits of this new environment for the organization's performance which is my bottom line?

IT Manager/CIO: The new information environment will provide the following benefits:

- Increased accessibility to applications, data, and systems for global users from multiple devices.
- Enhanced performance and information sharing of relevant and appropriate documents for password-protected/role-based access.
- Flexibility to respond to new requirements and technologies using dynamic allocation of computing resources.
- Resiliency for disaster recovery, business continuity or continuity of operations through large scale data centers and automation hosted off-site, in multiple locations that can be accessed from anywhere.
- Scalability means that computing does not require an upfront investment by the organization, and on-demand service provides users with the capacity that they need quickly and cheaply.
- Efficiency comes from request-driven, dynamic allocation of computing resources for a mix of workloads, easy procurement and billing, and visibility on the costs of services and their usage and performance.
- Standards, interoperability, and benchmarks allow for measurement of availability, latency, cost per processing unit, cost per storage unit, and many other factors.
- Security can potentially be enhanced by *staff specialization, platform strength, resource availability* and resilience, *backup and recovery, mobile endpoints, data concentration,* and *data-center oriented, and cloud-oriented identity management* [2].
- Innovation and high performance are facilitated through speed and affordability of IT, two-way multi-channel solution development, perpetual development and deployment, sharing and institutionalization of new approaches, and end-user driven solutions.

Business Leader: These are benefits that will enhance performance, but where are the cost savings that you anticipate?

IT Manager/CIO: Most of the initial savings will come from consolidation of data centers. The next largest cost savings will come from reductions in the number of IT staff needed in organizations to support the local IT infrastructure. As the

technologies progress, fewer local IT staff will be required because specialists will be able to manage more equipment, users, and applications centrally and individual organizations will not need them to secure locally based computers, servers, and applications. In government organizations, we may need to absorb the IT staff into other roles. With thin devices, the need for equipment refreshment will be much less frequent and expensive, and user licenses will vary with need. Enterprise solutions will reduce the costs at each organization.

Business Leader: OK, so what are the risks?

IT Manager/CIO: In a volatile environment change is constant, and with change comes risk. As a business leader you are involved with risk every day. Risk-taking is a necessity for any enterprise that seeks to survive and thrive in uncertainty. The identification of risk is essential so that appropriate counter measures can be considered. Risk management focuses on identifying, analyzing, and developing strategies for responding to risk efficiently and effectively. The goal of risk management is not to avoid risks at all costs, but to make well informed decisions as to what risks are worth taking and to respond to those risk in an appropriate manner [3]. The higher the potential value of a project, the greater the importance of identifying risks early to mitigate a risk's probability and to take advantage of potential opportunities.

Business Leader: From what I am hearing, the biggest resistance to cloud computing is related to security, trust, and privacy.

IT Manager/CIO: Security, trust, and privacy risks concerning cloud computing must be addressed throughout the transition to the new environment. Many of these risks are common to conventional IT systems and not unique to the emerging infrastructure, but some may be exacerbated in a cloud environment. These risks include inappropriate and unauthorized use of cloud computing applications; insecure application programming interfaces; malicious insiders; shared technology vulnerabilities; data loss/leakage; account, service, and traffic hijacking; and questions concerning the risk profile due to its unfamiliarity. On the other hand, moving to this new environment may assist in resolving or reducing some long-standing issues inherent in the current environment or provide better mechanisms to monitor and mitigate existing vulnerabilities.

The privacy of data is a continuing concern that must be addressed. Certain types of data may trigger specific obligations under national or local law. Vendor issues to be addressed include: situations in which organizations may be unaware they are using cloud-based vendors; due diligence as in any vendor relationship; customer responsibility for data security; service-level agreements to account for access, correction, and privacy rights; and during data transfer, cloud models that may trigger international legal data transfer requirements. Through a variety of mechanisms security and privacy issues must be addressed, including use of negotiated service-level agreements that spell out the contractual requirements of a service provider that meet organizational and privacy requirements.

An organization's security and privacy objectives will determine the degree to which governance, compliance, trust, architecture, identity and access management, software isolation, data protection, availability, and incidence response must be addressed. Options for different purposes exist for our

organization's transition to public, private, and/or hybrid clouds for different applications and data.

Business Leader: Any change in a large, complex, decentralized, distributed, and deployed organization requires the early and frequent engagement of key stakeholders. These stakeholders must be engaged in the risk management analysis because they are responsible to deliver on the mission. They must understand the potential benefits of the planned change, in this case the transformation to the new information environment, as well as its risks. Senior leaders across the enterprise must participate actively in the governance of the change initiative. Leaders must develop a sense of ownership for the initiative and seek to develop that same sense of ownership in users across the organization.

The benefits for organizational performance of a new information environment enabled by cloud computing are convincing. But transformation will be challenging. In my experience, transformation only succeeds when culture, strategy, vision, processes, incentive, and accountability are aligned and reinforce each other. We need to address cultural issues to facilitate new ways of thinking and behaving. We need to develop enterprise solutions that focus on our shared mission goals. Risk-avoidance behaviors must be replaced by risk management strategies to manage uncertainty.

Essential to the success of this transformation is governance, a system of explicit participation of stakeholders, processes, and approvals that lead, fund, and monitor the change initiative. Government leaders should take advantage of the government efforts to date, including pilots and policies, innovations and experiments, and advanced technologies being employed by other organization with similar goals. Change management planning must be thoughtfully and strategically developed, must engage senior leaders who understand and enthusiastically endorse its development, and must leverage the expertise of wide talents of technology and change experts and users across the enterprise. Risk management will need to be explicitly included in the change management planning process.

You have convinced me of the value of cloud computing as an enabler of a new information environment. It has the potential to advance the mission and business of our government organization. I commit to become one of its principal advocates and leaders of the governance processes. The change management process will require all of us to move away from the familiar and comfortable/uncomfortable system we know to a new environment. CIOs and their IT staff need to engage in creative destruction of the systems they have built and maintained, in order support this transformation toward higher productivity, business performance and decision making.

Remember Sisyphus who was mentioned in the introduction? He is the king who is continually pushing that boulder up hill and not making much progress. Transformation to the new environment enabled by the cloud will not feel like a boulder if we convince business leaders to lead the charge for enhanced performance of the mission at lower costs.

Let's get started.

References

[1] M.P. McDonald, and D. Aron, "Reimagining IT: The 2011 CIO Agenda," Gartner, ID Number G00210382, 1 January 2011.

[2] W. Jansen, and T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing," Draft Special Publication 800-144. Computer Security Division, Information Technology Laboratory, NIST, Department of Commerce, Gaithersburg, MD. January 2011.

[3] G. Choo, "It's a Risky Business." http://www.gantthead.com/content/article/18271.cfml, 2001.

Disclaimer

The views expressed in this paper are those of the author and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the U.S. Government.