

# Major Challenges Facing Government in Implementing Cloud Computing

*The Economist* (2008b) stated that “the rise of the cloud is more than just another platform shift that gets geeks excited. It will undoubtedly transform the information technology (IT) industry, but it will also profoundly change the way people work and companies operate. It will allow digital technology to penetrate every nook and cranny of the economy and of society.” IT executives must decide if the cost savings and flexibility/scalability to be gained through shifting data and functions to the cloud are worth the trade-off in terms of control and security (Schwartz, 2008a). Lohr (2009) points out that many IT executives in both the private and public sectors have been reluctant to jump on the cloud computing bandwagon due to “traditional corporate computing concerns like the security of data, reliability of service and regulatory compliance.” Indeed, many public sector IT executives like the idea of shifting data and applications to public clouds, but control, access, security, and interoperability issues will need to be resolved before their organization could make use of public clouds (Linthicum, 2009).

In this section, we will examine ten major issues facing government leaders in the shift to using cloud computing. They are:

- **Challenge One:** The Need for Scalability
- **Challenge Two:** The Need for High Reliability
- **Challenge Three:** The Need for Securing Data in the Cloud
- **Challenge Four:** The Need for Open Standards and Interoperability
- **Challenge Five:** The Need to Revise Procurement Practices
- **Challenge Six:** The Need to Resolve Potential Legal Issues
- **Challenge Seven:** The Need to Regulate the “Cloud Market”
- **Challenge Eight:** The Need to Redefine the Roles of the IT Workforce
- **Challenge Nine:** The Need to Assess the Return on Investment of Cloud Computing
- **Challenge Ten:** The Need for Government Cloud Coordination

## Challenge One: The Need for Scalability

Flexibility. It’s become a hallmark of successful strategies in the business world today, with sudden shifts in the overall economy and in specific markets becoming commonplace. As Erik Brynjolfsson, professor at the Massachusetts Institute of Technology (MIT) Sloan School of Management and the director of the MIT Center for Digital Business, observed, “The economy has become much more volatile, not just in the past year, but over the past 10 years. The ability to be agile in your infrastructure is what separates the winners from the losers ... cloud computing is one of the most important technologies that affect the ability to maintain that level of flexibility” (quoted in Cass, 2009).

In today’s environment, IT resources will need to become more flexible, agile—in other words, scalable—for all organizations. Cloud computing turns the economics of IT on its head, due to an unprecedented elasticity of resources. In everyday use, elasticity is commonly thought of not just as the ability of an object to stretch out when needed, but to also contract as necessary (think of a rubber band or a bungee cord). In computing terms, elasticity can be defined as “the ability of a system to dynamically

### ***The New York Times' Use of Cloud Computing***

In the relatively short time that cloud computing has been available, there have already been truly amazing examples brought forward by companies making innovative use of the scalability of on-demand computing resources. If you want a good illustration of the power of cloud computing in action, you need look no further than your doorstep (or bookstore) as to how the *New York Times* discovered the power of cloud computing.

In 2008, the *Times* took on the task of adding many years' worth of articles to its searchable web database to make them available for download. It sought to add roughly 11 million articles, published from the newspaper's founding in 1851 up through 1989. With its cloud computing offering, the Elastic Compute Cloud, or EC2, Amazon offers anyone—be they a large company or an individual—the opportunity to run applications or crunch numbers quickly and cheaply. To accomplish the *Times'* massive computing task, an IT staffer at the *Times* merely set up an account with Amazon Web Services with his credit card. *Times* staffers then began the tedious task of cutting the physical copies of the articles and scanning them into TIFF files. These files—approximately 4 TB (terabytes)—were uploaded to Amazon's S3 storage site; then, using its EC2 platform, the files were converted into 1.5 TB of Adobe PDF files, ready for use on the *Times* website. The job was done in less than 24 hours, using 100 LINUX machines. And the cost for all of this was less than five hundred dollars (Snyder, 2008; Gruman, 2008)! Derek Gottfrid, who is the senior software architect for the *Times*, commented that “it would have taken a month at our facilities, since we only had a few spare PCs. It was cheap experimentation, and the learning curve isn't steep” (quoted in Gruman, 2008).

Nicholas Carr (2009a) commented that “the *New York Times'* use of Amazon.com is a small but telling example of what happens when you radically democratize computing so that anyone has access at any moment to super-computer-type capacity and all the data storage they need.” This availability of computing processing and storage power on demand could have profound implications in everything from scientific inquiry (by making no problem too big to compute) to new enterprise formation (by drastically reducing the need for up-front investment in IT resources—and the people to support and maintain them) to public agencies (by making IT more affordable and available to governments at all levels and in all locales). Thus, we may be seeing a truly new era, wherein there is a “democratizing” of computing technology under way—bringing “the benefits of high-powered computers and communications to all” (Foley, 2009c).

acquire or release compute resources on-demand” (Langley, 2008). Under the cloud model, organizations that need more computing power dramatically increase their computer utilization without having to pay a premium for that ability. Say, for instance, that a company has large, batch-oriented processing tasks. It can run the operations far faster than previously possible and at no additional cost, “since using 1000 servers for one hour costs no more than using one server for 1000 hours” (Armbrust, et al., 2009, p. 1). This unique attribute of cloud computing is commonly referred to as “cost associativity,” and it allows for computational needs to be addressed far faster and far more cheaply than in the past. In short, cloud computing gives organizations—even individual users—unprecedented scalability.

In IT terms, scalability can be defined as “the ability of a computing system to grow relatively easily in response to increased demand” (Langley, 2008). Cloud solutions are ideal for situations where there is “spiking” of demand—sudden shifts from handling little or no traffic to having the need to handle huge

levels of traffic (Chan, 2009). In the private sector, this may be handling online sales on the morning of Black Friday sales on the day after Thanksgiving or allowing for online voting on a show like “American Idol” or “Dancing with the Stars.”

In the public sector, the analogous situations could be traffic going to either the Internal Revenue Service's website on April 14 (the day before federal taxes are due) or the Federal Emergency Management Agency website to apply for disaster assistance in the wake of a hurricane or flood. Certainly, one of the principal benefits of shifting to cloud-based applications, communications, and storage capabilities is in the area of disaster planning. When a disaster does occur, the off-site—and often out-of-region—capabilities of cloud providers to the affected governmental jurisdictions become an IT lifeboat—enabling agencies to more easily maintain operations during a natural or man-made disaster and more quickly recover to normal operational capabilities.

## Challenge Two: The Need for High Reliability

One of the principal concerns about cloud computing is the reliability question, and this is certainly a case where, when a tree falls (i.e., an outage occurs), everyone hears the sound. Unfortunately, worries over cloud reliability and availability—or specifically, the lack thereof when such instances arise—are not just theoretical.

There have been well-publicized outages of many of the most popular public cloud services, including Gmail and Google Apps (Worthen and Vascellaro, 2009), Apple's MobileMe service (Parr, 2008), and Amazon's S3 cloud service (Perez, 2008; Waxer, 2009). And, as Schwartz (2008a) astutely pointed out, when cloud service outages or inaccessibility occur, "most of the risk and blame if something goes wrong will fall directly on the shoulders of IT—and not on the cloud computing service providers." For instance, in September 2009, Gmail had its longest outage—lasting over 100 minutes. Such downtime for e-mail services can cast doubts in the minds of IT decision makers over the viability of the bigger proposition of replacing desktop functionality with functionality from the cloud (Gralla, 2009).

For private sector IT executives, there is a reluctance to shift core, mission-critical data storage or applications to public cloud environments, even if the cost savings and efficiency arguments are there, over concerns about the reliability and security of cloud offerings. Take, for instance, the case of the Princeton, New Jersey-based Educational Testing Service (ETS), which administers the SAT and other standardized tests. While ETS uses Software as a Service (SaaS) platforms from Salesforce.com and other vendors for noncore functions, the firm's chief information officer (CIO), Daniel Wakeman, recently expressed his reluctance to shift data storage and processing for the tests themselves to a cloud environment. This is in spite of the fact that, due to the highly cyclical nature of test administrations, scoring, and reporting around specific testing schedules throughout the year, ETS has an average server utilization rate of just around 8 percent, making the firm a prime candidate for acquiring computing resources on demand.

Wakeman simply stated that, due to security issues which have yet to be worked out in what he and other perceive to be an "immature market," ETS will monitor developments in the cloud marketplace and

"not (be) putting anything up there that we really care about" (quoted in Stedman, 2009).

One of the truths about cloud computing, as pointed out by Waxer (2009), is that in-house IT can rarely match the service levels provided by commercial cloud providers. For a cloud provider to offer a service level agreement (SLA) with "four-9s performance," it would be guaranteeing 99.99 percent uptime. Translated into "real life," four-9s availability translates into just 52 minutes of downtime per year. If there were more downtime or unavailability than that .01 percent, then the cloud provider would be liable for penalties or rebates. To assure this level of service, cloud service costs typically rise as the SLA escalates from three-, four- or even now some "five-9s" levels of performance (Waxer, 2009). SLAs have been criticized for not protecting cloud-procuring organizations from a loss of system uptime, but protecting cloud providers from financial and legal exposure after their failure to deliver. As such, they have been labeled as only applying "after the fact" and being a "vehicle to argue over" and likely mitigate (Golden, 2009b).

As discussed above, cloud providers typically guarantee a particular benchmark for the availability of their services through what are known as SLAs. Yet, for all the reliance on SLAs, there is misunderstanding as to what they really guarantee—and what can be done should a cloud provider fail to live up to its promises. In many instances, collecting on the rebate provided for in the SLA may not be a routine matter (Brodkin, 2009c). It also may not mean much if the outage comes at a critical moment, for which no amount of money can make up. As one commentator opined, "Frankly, I think SLA and \$3 will get you a coffee" (Krill, 2009). Still, as Golden (2009a) advised, avoiding cloud computing solely on the basis that SLAs invariably can't cover actual business losses from downtime or outages "is a rationalization, not a reason" for not engaging the cloud computing model.

For the government, SLAs may be especially vacuous if a data breach occurs and a law is broken—as the bar is raised much higher for a public sector client. As Chabrow (2009a) commented, in such instances:

The government doesn't have the luxury of just saying, 'Oh, give me my money back.' They need to follow laws that have been

specifically laid out to protect national security, to protect personal liberties; so, it's really not just a commercial transaction. They really need to understand the details within these infrastructures. It's not enough to say, 'Oh, yes, it's secure.' The government has to understand how it is secure, why it is secure, what are the risks. If the government can't see that, then it's very difficult for them to leverage that type of service.

Cloud providers invest a great deal in their systems to provide for reliability and assure that their services—and user data—will be available on demand. For instance, Amazon Web Services has a feature in its EC2 (Elastic Compute Cloud) dubbed “failover,” where, if a user's application fails to run in one of Amazon's data centers, a second center will automatically take over and run the application (Ricknäs, 2008). There are even early versions of cloud applications that can be run offline—in the absence of a network connection (Naone, 2009). Developments in this area would enable cloud computing to move to the edge of the network and be functional in remote areas where there is spotty connectivity—defeating one of the exclusionary rationales for not making use of cloud-based offerings.

### Challenge Three: The Need for Securing Data in the Cloud

John Garing, the Defense Information Systems Agency (DISA) CIO and director of strategic planning, characterized the federal government's dilemma as the classic case of the “irresistible force versus immovable object,” where “the irresistible force is the incredible thirst for collaboration and information-sharing that Web 2.0 tools and many young people have brought on board, and the immovable object is security” (quoted in Harris, 2008).

Security is undoubtedly a hard metric to quantify. And, all too often, from the perspective of Golden (2009c) and other observers, the IT community has a somewhat damaging tendency to treat all risks—whatever the real nature of them—as the very worst-case scenario and not judging the true impact—and likelihood—of their occurrence. And today, many security experts believe that the notion of putting more data and more applications on the Internet via the cloud model could present vast new opportuni-

ties for criminal activity through identity theft and misappropriating intellectual property, hacking, and other forms of malicious activities (Bailey, 2009).

The degree to which *any* organization engages in cloud computing—whether outside or inside its own “four-wall” environment—will certainly depend on its need for security (North, 2009). Thus, with heightened security concerns, how to make cloud computing secure is one of the biggest issues for making it viable for the federal government—or for any government agency. As with prior shifts in IT with the advent of the Internet and the web, the introduction of e-mail, and the explosion of social media, their growth and adoption rates have been slowed by initial fears—some justified and some very unjustified—over security concerns and the loss of control over data and operations (Kelton Research, 2009). Indeed, analogies have been drawn between the advent of cloud computing today and the introduction of wireless technologies a decade ago. As Ron Ross, the National Institute for Standards and Technology's (NIST) director of security, observed, “When wireless came along, we didn't really know a lot about how to protect it, but we developed that understanding as we went forward, and now we do a pretty good job of protecting wireless” (quoted in Beizer, 2009c). However, Wyatt Kash (2008), editor-in-chief for *Government Computer News*, warned that the shift to cloud computing could be slowed by what he termed as “a darker cloud of Internet security vulnerabilities.”

Privacy and security questions will need to be addressed as public data and applications move into a cloud environment. Adrienne Thomas, acting architect of the United States, stated, “It's a very big issue for government, in terms of someone else to have control of our stuff” (Hoover, 2009c). Yet, as Arun Gupta, a partner at Columbia Capital, a venture capital firm, who worked with Vivek Kundra during his time as chief technology officer (CTO) for the District of Columbia observed, in order to succeed today, “You have to have the confidence to say, ‘I don't need to control everything.’ That's very much a Web 2.0 mentality. Is that the panacea to everything? Probably not. But it's a step in the right direction” (quoted in Hart, 2009b). Linda Cureton (2009), CIO of NASA's Goddard Space Flight Center, told IT decision makers in government that it is imperative when considering a cloud-shift: “Don't confuse control and ownership with security and viability.”

Kaplan (2009) categorized the widely held perception that cloud computing and SaaS applications were less secure and less reliable than applications housed on an organization's own network as nothing less than a "myth." Indeed, cloud offerings may be significantly more reliable than an organization's internal offerings (Worthen and Vascellaro, 2009). The difference is that, when a company's e-mail server crashes or a power outage disrupts operations at its data center, these internal failings do not make media headlines, as is the case anytime there is an outage or data breach with a Google, an Apple, or an Amazon cloud offering. As Kash (2009) framed the issue, large-scale cloud providers are oftentimes more secure than a government agency's or private sector company's internal IT operations, simply because they have the "talent, resources and focus" that their customers—and their smaller counterparts—do not have. Still, IT executives stridently believe that their own hosted systems are far more secure than cloud-based resources (Foley, 2009d), and public sector IT managers stridently believe that their internal operations are more secure than those that a private sector vendor could provide (Brodkin, 2009b). Still, as Gardiner (2009) observed, "hard-liners see the very concept of the cloud as a deeply unreliable security nightmare."

Musco (2009) characterized the need to retain control and protection of sensitive, private data, in an age of information sharing, the "Catch-22" for government IT with regard to cloud computing. Data security questions are, by definition, dependent on the nature and sensitivity of the data involved. Ron Ross, NIST's director of security, observed that it is important to consider the sensitivity of the data in question and to develop and employ "a range of security controls (that) will be appropriate for differing levels of data sensitivity" (quoted in Condon, 2009a).

One of the complicating factors in the shift to a cloud computing environment will be federal requirements for agencies to certify the security of their IT contractors' systems. There are presently no cloud-specific security standards in place. From the perspective of NIST's Peter Mell: "Compliance is going to be tricky in the cloud space for several reasons, but one reason is that clouds are likely to use new security technologies that aren't well understood or widely adopted, and that will make it difficult to prove the required level of security to auditors

and to authorizing officials" (quoted in Chabrow, 2009b). Some have questioned whether the federal government would be precluded—from a regulatory standpoint—from using cloud-based services for such reasons. In fact, John Curran, CTO and chief operating officer of ServerVault, commented, "For many agency applications, stringent compliance requirements in areas such as privacy, financial controls, and health information will preclude use of public clouds, regardless of the actual security controls of the provider" (quoted in Foley, 2009e). Analysts have already voiced concern that cloud providers methods of logging activities and document reads/access are presently insufficient for meeting the needs of government agencies to assure their compliance through audit controls (Westervelt, 2009).

Analysts have stated that one of the benefits for small companies is that they may, in fact, be able to raise the level of their computing security by moving more data and applications to the cloud. This is simply because cloud providers will have more resources to spend on security for their operations than can most individual firms. Plus, their investments in security can be spread over their entire present—and prospective—client base (perhaps hundreds or thousands of firms), producing far greater results in improving computer security than an individual firm's investments in such efforts (Schwartz, 2008a). The same principle will hold true for government clients as well, especially those at the state and local levels. Yet, analysts have said that this may also be true even at the federal level, as large cloud providers—whose business depends on secure operations—may provide better security than internal federal operations (Hart, 2009a).

For their part, cloud providers have been characterized as addressing such security concerns by going "over the top" with their physical and data security measures, which one writer labeled as measures that could "easily outdo anything ever seen on *Mission: Impossible*." He cites the fact that Salesforce.com's data center employs "five levels of biometric hand geometry scanners and even 'man trap' cages designed to spring on those without the proper clearances" (Gardiner, 2009). This is evidence that cloud providers are very much aware of and attuned to both their clients' concerns in the security area, and the legal and regulatory risks that are being taken on by both the client and their firm

### Can Cloud Computing Pose a National Security Risk?

As ever-greater amounts of governmental and private sector firms' work is shifted to cloud computing, could this shift in the locus of computation indeed be creating a national security risk? Cohen (2009a) noted, "Cyber-threats against the country and the government are growing exponentially, and the desire to connect agencies and make government open, transparent and interoperable makes it easier for hackers to carry out their attacks—(thus) will openness and interoperability make us as a nation less secure?" He also went on to note that government will have significant interest in protecting cloud resources for the private sector and individuals as well, noting the huge economic impact and disruption that can occur if a major cloud resource, such as Gmail, were to go down for an extended period of time or be lost forever.

Such risks are not without precedent, as the government of Estonia was hit by a well-coordinated denial-of-service attack—suspected to be Russian in origin—during a period of tension between the two nations in 2007 (Kirk, 2007), and during Summer 2009, several agencies in the U.S. government and sites in South Korea were cyberattacked by what was widely believed to be a scheme conducted by the North Korean government (Williams, 2009). Such a risk has led Carr (2009b) to label this as the threat of a "Cold War 2.0"—and it is certainly an area where federal policymakers need to be concerned.

by accepting a sizable portion of the client's IT operations (Golden, 2009c).

What are the other benefits of cloud computing in the security area? One of the best ways to improve security is to have a single point of access, controlled by the organization and mandating that users follow their procedures and policies for access privileges. However, while such access controls return power to the client, they may well serve to defeat some of the robust advantages for remote access fundamental to the cloud computing model (Jackson, W., 2009). A recent study from researchers at the University of Michigan showed that, by shifting virus protection from individual PCs to the cloud that connected them by raising the level of protection to the network, the ability of antivirus software to detect viruses and malware was significantly improved (Greene, 2008).

Finally, cloud computing is also a relatively quick and easy solution to the significant problem of laptop theft, which poses a very real, intransigent security and financial headache for IT managers (Wyld, 2009). This is because, should a user lose his or her laptop, there would be no security threat, simply because the data would reside in the cloud rather than on the machine itself (Gardiner, 2009). In fact, some have said this would actually mean that cloud storage would increase security for the federal government by reducing the security risk inherent with the hundreds of thousands of laptops in employee possession both inside and outside of federal facilities (Hickey, 2008b).

In the final analysis, as Golden (2009c) observed, those who view cloud computing as too risky may be "overly optimistic" in their view of how well their own security and risk management efforts work—both in reality and in comparison to the cloud model. He remarked, "This attitude reflects a common human condition: underestimating the risks associated with current conditions while overestimating the risks of something new. However, criticizing cloud computing as incapable of supporting risk management while overlooking current risk management shortcomings doesn't really help, and can make the person criticizing look reactive rather than reflective."

### Challenge Four: The Need for Open Standards and Interoperability

Over the roughly 60 years since modern electronic computing came about, buyers of IT have had to be concerned with the very practical question, "Am I going to be stuck with *this*?" Whether *this* referred to an operating system, a version of software, or a type of computer, this could make the difference between having a "white elephant" system that would be obsolete and isolated or a system that could work with the latest and greatest technologies as they invariably supplanted what you just bought or what you just signed a contract for. Thus, from the original mainframe model of computing through the preponderance of Microsoft operating systems and its Office Suite on desktops and the database dominance of Oracle and SAP, interoperability and "lock-in" have both been major concerns for IT users, buyers, and administrators (Hamm, 2009b).

Today, cloud computing has been compared to the early days of the Internet, where CompuServe and America Online were “silos communities” that could not allow for interoperability or easy user switching (Naone, 2009). Knorr and Gruman (2008) described the current state of affairs as more accurately being “sky computing,” due to the fact that users—be they individuals or organizations—today largely do not plug into a single cloud, but rather multiple, isolated clouds that must be entered into separately.

Cloud computing may indeed provide a standardized foundation for computing across organizations. This is because, with the vendor-controlled platform, rather than one that can be modified on-premise, there will be a more standardized interface and a more stable environment in a SaaS environment (Schwartz, 2008b). From the perspective of Kaplan (2009) and other industry analysts, “a high level of customization can be counterproductive.” Most of the public cloud applications are publicly available for use, but are not open source in nature. Blauer (2009) termed such software as being “free but not open.” According to his analogy, when you do not have access to the source code, “an important distinction is (to be) made between free and open, the former being akin to free beer, and the latter akin to free speech.” While open source will be an alternative to cloud applications, cloud software needs to mostly be standardized—“to get the benefits out of the cloud, you really want to rely on the cloud service as it exists, because if you get unique in the cloud, all of a sudden it’s not the cloud—it’s your own little outsource bank” (Kash, 2009).

Indeed, standards issues may lead not just to greater interoperability and portability, but perhaps something greater. There is already talk of the development of an “intercloud,” which *The Economist* (2008e) described as “a federation of all kinds of clouds, in the same way that the Internet is a network of networks.” As Hall (2009b) observed:

When a new approach to technology takes off like cloud computing is today, the last thing you want to do is hamper its development by instantly weighing it down with new standards. One of the wisest ideas in the *Open Cloud Manifesto* is the argument to use, wherever feasible, existing standards. But it does not follow that, where existing

standards do not exist, new ones need to be developed, at least not immediately.

One of the primary concerns regarding cloud computing that government IT executives consistently express is a fear of being locked into vendors, due to the high switching costs—both in dollars and in time and effort—that would be incurred when switching between cloud computing providers (Hall, 2009c). Indeed, Robert Ames, the deputy CTO for IBM Federal, believes that “the government has a fear of lock-in,” and this fear of being tied to a specific provider’s systems and pricing is one of the overriding factors that is holding back the federal government’s adoption of cloud-based technologies (Hall, 2009b).

Brandel (2009a) astutely made the distinction that vendor lock-in is not a unitary concept, as the varying types and categories of cloud offerings each have different levels of commitment and lock-in. Yet, even while tying their organizational computing resources and data to “traditional” platforms such as Microsoft, SAP, and Oracle, IT leaders continue to express heightened concern over lock-in with cloud computing. This is due to the simple fact that the data is not hosted on their own systems and within their own premises. Still, one must consider that with any IT choice—be it even in investing in one’s own systems hosted on-site—there are lock-in and data migration considerations. In fact, lock-in may be greater with internal systems than cloud systems—even in today’s unfolding cloud marketplace (Brandel, 2009b).

It is also critical to deal with what happens at the end of a cloud computing contract, whether the contract involves a public sector agency or a private entity. As Brandel (2009a) advised, it is imperative that IT executives insist that their contracts with cloud providers contain specifics on how to end the relationship and safely migrate their data either to another cloud provider or back in-house.

Thus, one of the principal ways that government can help to foster the overall growth of cloud computing is to support the establishment of standards that will ensure common architectures and portability of data and files. Rayport and Heyward (2009) advocated that the federal government should be an active participant in the standards-setting efforts, such as the Open Cloud project, and they stated

that “ideally, what governments can do best is clear the road, not pave it.”

Standards are vital to growing the overall cloud computing and infrastructure market. From the perspective of Winston Bumpus, president of the Distributed Management Task Force (dmtf.org), an industry-led effort to establish standards in the cloud computing market, “You need standards to avoid vendor lock-in.” Yet, while vendors may ultimately cooperate on standards efforts, the lack of standards today is a short-term benefit to cloud providers, as it gives cloud vendors greater leverage by making it harder for customers to leave them. Thus, the primary driving force for the establishment of standards will come from customers, as standards will help overcome the real and perceived fears of vendor lock-in.

## Challenge Five: The Need to Revise Procurement Practices

In the governmental space, IT outsourcing has become a well-established practice. However, as Jimmy Lin, an assistant professor of information studies at the University of Maryland observed, “The government may be outsourcing functions to contractors now, but this (cloud computing) takes it to a whole new level” (quoted in Hart, 2009a).

Certainly, one of the challenges that will have to be dealt with as the switch to greater use of cloud computing in government occurs will be government’s contracting processes. New rules and regulations, some of which may even preclude the use of cloud computing in select instances, will need to be changed to be more cloud-friendly and encourage the savings and efficiencies that can come from this new model of IT.

Federal CIO Kundra has made IT procurement reform a top priority, as he is asserting that it is important for federal leaders to “recognize we can’t treat technology procurements in the same way we do buying buildings” (quoted in Weigelt, 2009a). One of the themes consistently being promoted by Kundra is the need to have a common platform or infrastructure across the federal government that will make it easier to leverage cloud resources and take full advantage of this paradigm shift. Otherwise, what many analysts fear is a continuation of the

### Options for Outsourcing and the Cloud

Outsourcing has always been a part of any organization’s IT decision making, as by outsourcing non-core functions, executives are able to more fully concentrate on strategic priorities and core competencies (Ross and Westerman, 2004). Tech pioneer Geoffrey Moore (2000) developed the concept of core versus context IT activities in organizations. According to Moore’s typology, core functions help provide the organization’s competitive differentiation and span the organization to connect to its external constituencies, while context functions are typically internal in nature and help support the core activities. In an interview, Moore quipped that, if executives are “caught up in managing old context stuff and you don’t find a way to get that stuff out of the company, you have trouble turning the boat,” and thus, it is crucial to concentrate on the core functions to promote long-term success (quoted in *Business Week*, 2000).

We may, as Collett (2009) predicts, be quickly moving into “a world where everything is provisioned” in computing. In the realm of deciding which activities to keep internal and which to potentially shift to the cloud, Schwartz (2008a) offered the following “rules of thumb,” based on Moore’s core-versus-context framework: “If the business practice is context and non-mission-critical, then always put it in the cloud. If it is context and mission-critical, it is likely you should make it cloud-enabled. However, if it is core and non-mission-critical, you may want to think about keeping it behind the firewall; if it is core and mission-critical, then definitely keep it behind the firewall.”

problems of information silos and unnecessary redundancies and their attendant costs. As Condon (2009b) noted, “Unless you think strategically about how the government works and wants to work, instead of having 150 data centers, we’ll have 150 different clouds.” Yet, the government is not a “one size fits all” institution, and it is likely that the various needs and interests of agencies will require unique solutions—even if coming atop a shared architecture to some degree or another.

Indeed, one of the challenges going forward will be to make acquiring cloud-based services as easy as possible to obtain. To that end, Kundra has announced a plan to work with the General Services Administration (GSA) to establish a “cloud computing storefront.” According to Kundra, the storefront

will “allow the agencies to quickly find cloud solutions” (quoted in Stegon, 2009). This initiative resulted in the creation of Apps.gov in September 2009 (see page 25). According to Kundra, “the key is to make [cloud computing] available to the federal government in a way that’s easy.... We’re moving from this notion of ‘here’s a schedule’ to the notion of ‘here’s a platform that can be provisioned in real-time’” (quoted in Hoover, 2009i).

With these changes in motion, some have suggested that, with federal contracting currently not geared toward purchasing IT on an “as-needed” basis, it will be incumbent upon cloud providers to educate lawmakers as to cloud computing’s benefits and the changes in contracting rules that will be necessary to facilitate such procurements (Gross, 2009d). Current federal guidelines are not geared toward purchasing computing on a pay-as-you-go, as-needed basis (Gross, 2009c), and at all levels of government, annual budgeting practices tend to emphasize fixed costs to match fixed levels of funding, rather than variable pricing—even if it is cost-effective to do so (Miller, J., 2008). There will thus need to be vast changes in not just the language, but the *mindset* of contracting for computing services. For while IT administrators look at capacity and systems, end users look to performance. As Jackson (2009d) put it, the key metric will now become: “When I sit down at that computer, do I see the functionality I need?”

Take, for instance, the challenge faced by the U.S. Department of the Interior’s National Business Center (NBC). The NBC provides a variety of business services to other federal agencies, and it hopes to add a variety of cloud computing offerings to its slate of services. Yet, it is challenged to do so from a contracting perspective—needing vendors to offer more “government-savvy contracts.” To that end, NBC Director Doug Bourgeois commented, “How can the private sector infrastructure providers provide me with a business model that’s pay-as-you-go? My customers are only going to pay for what they can use. I need to purchase infrastructure and technology under the same model, so it’s truly a shared-risk partnership” (quoted in Gross, 2009d).

**Pricing.** How to price (and how to negotiate and evaluate) cloud computing contracts will become a huge issue over the next decade as more and more corporate and governmental computing shifts to

## Where in the Clouds?

Where does data reside in the clouds? For redundancy, client data often resides in multiple data centers—and perhaps in different countries. For example, Google does not disclose the exact location of where—physically—a Google Docs document might be housed in one of its massive data centers. This would be “a major deal-breaker” for government contracting requirements calling for pinpointing the physical location where data is housed. Thus, with the risk of a data breach being network-based rather than physical security-based (as it is far, far, far more likely for data to be wrongfully accessed or deleted via either remote or internal access than for the server it resides on to be physically stolen or tampered with), as Jackson (2009c) astutely pointed out, in an age of ubiquitous connectivity, “access, rather than location, may be the better way of thinking about things.” Still, with developments in virtualization and multitenant architecture, cloud providers can begin to physically separate customers’ data in the cloud (Schwartz, 2008a). Public sector clients may thus well require—or be required by new or newly interpreted regulations—to have their data and applications physically segregated (via virtualization or on different servers) from the private sector clients of cloud providers.

The actual “where” in the cloud computing equation *does* become an issue, however, when dealing with government data and functions. For the federal government, there will certainly be restrictions that data storage and processing actually take place within the U.S., precluding the use of cloud providers that might move offshore similar private sector work to data centers located in foreign countries—a development that will continue to grow over the coming decade. (Andriole, 2005; Hall, 2009d). This has likewise been seen in Canada, where national and provincial governments have been slow to adopt cloud computing—due to the hesitancy and Canadian Homeland Security restrictions against putting Canadian public data in foreign data centers—with most major cloud providers being U.S.-based (Rocha, 2009). Likewise, some European governments and companies have expressed concern about working with U.S. based cloud computing providers out of concern that their data—housed at least partially on American soil—could be subject to governmental review due to the provisions of the Patriot Act (Mitchell, 2009). Finally, in order to encourage economic development, states and major cities may require cloud providers to either manage operations in government data centers or to even locate data centers within their jurisdictions—so that the money and jobs stay in their own local area!

cloud providers. Cloud pricing models that are based on usage (the pay-by-the-drink model) could be confusing—and even off-putting—to IT managers and organizational executives. As Allan Leinwand, a partner with Panorama Capital, commented, “You’re talking about units that people don’t normally think about. CPU hours: that’s not something I go buy. I buy a blade server, and the hours are infinite, they’re mine. Even if an IT pro finds it easy to understand CPU hours, a CFO might not. Try to explain to your CFO how many CPU hours you’re going to use in the cloud, and see if they care” (quoted in Brodtkin, 2009c). Furthermore, those entering cloud computing contracts expecting considerable cost savings could experience the “sticker shock” that many of us do with our cell phone bills; if utilization is far greater than anticipated, so too will be the tab for that computing power used from the cloud provider. In other words, metered pricing works well—but only if based on considerable planning, analysis, and understanding of the up- and downsides of consumption-based cloud pricing models.

Some have also criticized the current pricing models for cloud storage, insisting that it makes little sense to charge the same amount to store large amounts of data over a long-term basis. This is due to the fact that storage costs are likely to continue their steady, unabated decline into the future. They argue that unless cloud storage providers develop new pricing and storage models to recognize the different needs clients have for the security and accessibility of their data, the attractiveness of cloud storage may pale versus the declining costs for in-house storage (Brandel, 2008). There also will have to be efforts made to educate procurement staffers on consumption-based contracting and the need for sharing best practices and lessons learned as more experience is gained across the board in this area.

**Vendor Concerns.** Certainly, one of the principal concerns for anyone using the cloud is the financial and organizational stability of the cloud provider. There is a customer risk in the possibility that the cloud provider could cease operations—and then what is to happen? Whether it is an individual storing pictures in the ether or an organization storing files with a cloud provider, if that firm goes bankrupt, the data may be irretrievable (Brockman, 2009). Thus, vendor financial stability is certainly a concern for public sector buyers of cloud services and storage.

Financial concerns are not the only eventuality that could prove troublesome or even fatal: What if a cloud provider stops operating for another reason—say, the destruction of a data center by a natural disaster (without a redundant secondary backup of their housed data)? Likewise, some have expressed concern that, for providers such as Amazon, their cloud operations are not part of their traditional, core business (Golden, 2009c). This is not to say that, as the cloud model takes off, the cloud portion of their operations will not likely become a much more significant part of the cloud provider’s revenue and business model. However, there is always a potential risk when dealing with a firm whose primary line of business is not the area that you are contracting to become dependent upon.

**Compliance.** The greater automatization and standardization embedded in cloud processes may free up many, many work hours of senior and midlevel IT managers from focusing on compliance issues to other, arguably more productive, uses of their time. Still, some are concerned that some cloud providers will be unwilling to open up their operations for the security vetting necessary for federal contracting. However, it is likely that, once contracting guidelines are refined and cloud providers know specifically what they will need to do to be certified and accredited, they will be more than willing to go through the scrutiny, based on the potential size of contracting to provide cloud services to the federal government (Chabrow, 2009a).

## Challenge Six: The Need to Resolve Potential Legal Issues

Data handling will invariably be complicated by the cloud. When considering moving data to a cloud storage provider, it is important to remember the admonition of Damoulakis (2009), who observed: “Like a diamond, a piece of data, once created, is forever. It is typically stored, backed up, replicated and, perhaps, archived (all of which require more storage). But the likelihood that it will actually be purged is very low.”

When dealing with government data, records may need to be retained for longer periods of time and be made accessible for Freedom of Information Act (FOIA) requests. Likewise, information that was formerly only available through formal FOIA requests

may now be readily available online through the Data.gov portal and, perhaps, through cloud-based federal resources that could speed compliance (N. Thompson, 2009; Aitoro, 2009b). There have also been issues raised as to whether corporate data would be protected from unwarranted search and seizure by government investigators and law enforcement when the data reside on the provider's servers in a SaaS environment, with legal analysts generally concurring that data hosted outside an organization's four walls is more open for sharing and investigation (Westervelt, 2009). All of this could lead to a whole host of legal and security issues for private sector firms, as well as for governmental entities both relying upon and/or investigating the clouds.

As IT functions and data are shifted to cloud computing, there are significant legal concerns that impact both the private and the public sectors, far beyond what can be addressed in this report. For instance, while for-profit organizations must comply with Sarbanes-Oxley regulations governing corporate financial reporting and record keeping, both the private and public sector face compliance issues with the Health Insurance Portability & Accountability Act (HIPAA). According to analysts, HIPAA does not specifically have any language precluding the use of cloud services. However, sections 164.308 and 164.314 of the law do require an organization to obtain assurance from any third parties involved in its data operations that they can properly safeguard the data (Schwartz, 2008a). Also, what happens with "multitenancy"—if a cloud provider's IT resources are used to host government data and applications side by side with private elements (Joch, 2009)?

There are several existing federal laws that may inhibit the adoption of cloud computing by the federal government. First, there are concerns as to how to conduct cloud computing under the Federal Information Security Management Act (FISMA). Analysts believe that cloud-based storage and application hosting can be legally conducted by private vendors, but FISMA compliance will be costly and complicated (Gross, 2009c). The NIST has determined that existing FISMA regulations cover cloud computing, and it cautions that cloud data storage practices and the "fuzziness" of cloud computing boundaries could make FISMA-required "snapshot audits" difficult to perform (Joch, 2009).

### **"Information Malpractice"**

There are rumblings that cloud computing may provoke a whole host of legal concerns—and liability. At the Interop 2009 Conference, Drew Bartkiewicz, a former high-ranking executive for Salesforce.com and now the vice president of cyber risk and new media markets for The Hartford, coined the term "information malpractice" to describe the possibilities for legal action stemming from cloud computing, declaring that "data is the new oil" because it offers both tremendous value and tremendous liability" (quoted in Evans, 2009, ).

Certainly, policymakers at all levels of government will need to examine the potential areas for legal action stemming from data loss, data breach, and data/application inaccessibility from cloud computing. With the rapid evolution of this technology, it is likely that such policy actions will be doomed to be behind the tech wave. However, such actions should be made in a coordinated fashion and strive to protect rights, while not inhibiting the beneficial uses of the technology. However, with greater reliance on centralized data centers and data repositories, the scale involved with cloud computing could make wrongful actions—and potential recoveries—far larger in scope than in traditional, "four-walled" computing environments.

In the cloud computing environment, legal concerns are elevated even more, and the office of the federal CIO is working with Congress to resolve them (Corbin, 2009). Many believe that FISMA reform will be the key element to enabling federal adoption of the cloud model, and that a revision to the 2002 law should be made to specifically address nascent technology such as cloud computing (Chabrow, 2009a). From his perspective, CIO Kundra sees FISMA compliance as a key element to cloud computing moving forward. He recently stated his vision: "Today, every agency has to get their own [FISMA] certification and accreditation, even if they are using the same set of technologies. Imagine how much money we could save if we were able to have a central place where you could get certification and inherit those rights" (quoted in Hoover, 2009i).

The federal government will also have to deal with the Privacy Act, which almost all agree needs to be updated to deal with the change from paper files to electronic files existing in relational databases. Leslie Harris, president and chief executive officer of

the Center for Democracy and Technology, lent her perspective. She said, “I think we all know that that law is severely outdated” (quoted in Corbin, 2009). Likewise, the federal government will be challenged to deal with FOIA requests as more data moves into the clouds—particularly if data are stored both on internal servers and on multiple cloud platforms operated by multiple providers (Beizer, 2009a).

In the final analysis, Congress will need to streamline decades-old electronic privacy and data protection regulations to conform to today’s computing realities—and to prepare for tomorrow’s. As Golden (2009d) points-out, not only will inaction inhibit governmental use of cloud computing, but wider adoption of cloud-based models in the private sector as well. This is due to the fact that IT and corporate executives legal concerns may well serve to trump all the economic and operational arguments for moving to cloud computing.

Similar legal questions will likewise impact state and local governments, as well as governments abroad. Thus, one of the key motivators for developing cloud interoperability and search ability will be public sector needs for compliance and data integrity/privacy assurance.

## Challenge Seven: The Need to Regulate the ‘Cloud Market’

Where does the growth of cloud computing take us? Some have speculated that, ultimately, the concentration of resources and power in the cloud leads us down dangerous paths. As Jaeger, et al. (2009) observed:

Cloud computing represents centralization of information and computing resources—quite contrary to the imagery that the label evokes. Centralized resources, by their very nature, are easy to control, by corporations that own them and governments whose jurisdictions they are under. This less-discussed fact represents a ‘darker’ or ‘stormier’ side of cloud computing and presents a danger to open information-based societies if the issues are not carefully considered.

Some have forecast that we may be headed to a future where there are fewer and fewer companies,

or as Kelly (2008) imagined, a single “planetary computer” that anyone around the world would be able to tap into from any device. Indeed, Carr has proposed that we are indeed heading to a “world wide computer.” In an interview with *Wired*, Carr stated, “IBM founder Thomas J. Watson is quoted—possibly misquoted—as saying the world needs only five computers. Is it true?” He [Carr] went on to say that “the World Wide Web is becoming one vast, programmable machine.... Watson was off by four” (quoted in Reiss, 2007). Carr believes that “we’ll probably see some kind of oligopoly, with standards that allow the movement of data among the utilities similar to the way current moves through the electric grid” (quoted in Reiss, 2007).

O’Reilly (2008) has warned that, due to the economies of scale and scope involved, cloud computing could lead to “a huge monopoly.” However, he also cautioned that the ensuing competition in this area could make “Windows versus Apple” look like “kid’s stuff.” Thus, in the near term, competition may well make cloud-based applications and storage even more attractive on a cost basis to potential enterprise customers. As such, this area needs to be monitored closely by governmental authorities to assure competition and choice among cloud providers.

Over the long term, any such consolidation in the emerging cloud services industry could be harmful—even threatening—to the economy, and as such, must be monitored by governmental interests. It is not just for the sake of preventing monopolization for public policy reasons, as more and more consumers and small businesses—and governments—will be dependent on the infrastructure offerings of large cloud providers such as Apple, Amazon, Google—and on the horizon, certainly Microsoft (Naone, 2008a). Erickson (2009) warns that some in the IT community have concerns that cloud computing might cause a new “Big Data” sector of the economy (comprised of firms such as Google, IBM, Amazon, and Oracle) to greatly expand.

Yet, cloud computing will invariably lead to a more vertically integrated structure in the computing industry. This has led legal and industry analysts to predict that just as in prior computing eras there were antitrust concerns and actions brought by the Justice Department against Microsoft and IBM,

similar concentration and market dominance could put Google—or another dominant market player that might emerge—at risk of antitrust actions in the next decade (Vogelstein, 2009).

In this fast-moving area, established regulatory models and practices may well need to be adapted to keep pace with the changing computing paradigm. As Nicholas Carr observed:

There's a danger of too much of this very important infrastructure falling into the hands of too few companies. It's critical that there continues to be competition both at the level of the utility and of component suppliers to the utility. Don't think hardware and software companies will go away; they'll just shift from supplying the user to supplying the utility company. So it's critical at the highest level to ensure strong competition between all those parties. Eventually, as with electricity, it may require the government moving in to ensure that there isn't too much consolidation (quoted in Melymuka, 2005).

Market mechanisms may also play a role in guarding against a true monopoly/oligopoly from developing in the cloud computing market space. For one thing, much of the cloud computing market (storage, simple SaaS, Infrastructure as a Service, Platform as a Service, and e-mail) may be in the areas that are commodity-like in nature, and thus, low-margin businesses. Also, because there will be many firms that will—out of choice and necessity—operate private clouds; they will be operating largely independent of the market conditions in the public cloud marketplace for their internal operations. Further, as such firms find they will likely have excess capacity, this surplus could be traded/sold through exchanges and brokerage-type operations. Such models are likely to develop in the very near future (Cass, 2009).

Finally, especially if megasized, market-dominant cloud providers do emerge, there may be a need for additional regulation. Based on the banking regulation model, there will be a role for regulations to ensure that cloud providers have enough “reserve capacity” to meet their customers’ demands, even in times of extreme utilization (a natural disaster or other emergency could provoke the equivalent of a computing “run on the bank” for capacity). Likewise,

as companies—and even federal agencies—are both users and providers of cloud services (much of what has been proposed by the GSA, NBC and DISA is about becoming cloud providers for agencies, outside of their primary scope), there may need to be guidelines and oversight as to whose needs are met first—the provider’s internal needs or those of their cloud customers (Greenberg, 2009a)? These are very good points that will most assuredly need to be addressed in the coming years as cloud oversight becomes a real issue. If not, we could well face the prospect of what Greenberg (2009a) terms a “cloud collapse” that could send the government—and the economy—reeling in the event of a major cloud provider failure without adequate procedures in place to address user needs and concerns.

## Challenge Eight: The Need to Redefine the Roles of the IT Workforce

Resistance to cloud computing from users is likely to be limited, so long as they can count on the same type of IT resources as they have had in the past. There will, undoubtedly, however be some resistance among the IT workforce to the advent of cloud computing. Traditional IT staffers are likely to be the most resistant, while those with experience with web development are likely to be supportive of cloud efforts (Gruman, 2008). Gardiner (2009) is among those who believe that the rising generation in the IT workforce—comfortable in their use of and reliance upon a whole host of web-based tools and services—will be more willing to shift operations and data to the cloud than will be the current generation of IT decision makers. They will likely see their older colleagues’ concerns about reliability and security issues regarding the use of cloud computing as “exaggerated and quaint.”

Many in IT may also perceive the shift as not just changing what they do, but as a threat to their very jobs. Martha Dorris, deputy associate administrator for the GSA’s Office of Citizen Services and Communications, commented that the biggest issue in her agency’s changeover of the USA.gov web portal to a cloud-based platform was that “our technology team did not want to give up the servers.” She observed that, in the end, “this isn’t a story about technology. It’s a story of culture” (quoted in Towns, 2009). As we have seen with so many technological shifts that have previously occurred, it is essential to

gain cultural buy-in from employees to get them to do something differently, as it is absolutely essential that “cultural change must accompany the technology shift” (Babcock, 2009). Indeed, many in IT will have to overcome the idea of data and applications not residing within their realm of control within their own four walls.

It is thus highly likely that, as with other major technological changes, the most important issues to be resolved will be people-based, not tech-based. As Patrick Stingley, CTO of the Bureau of Land Management, stated, “You have a culture that needs to change and to embrace the cloud and embrace the concept of sharing. Cloud computing is a shared service; we need to learn how to share. It’s not a hard concept, but we can’t agree how to do it” (quoted in Erlichman, 2009).

According to Kaplan (2009), many IT professionals are growing more receptive to the concept, as these cloud computing tools may in fact make their jobs better by freeing them from the “day-to-day hassles” of maintaining software. Jerry Hodge, senior director of information services at appliance maker Hamilton Beach, commented that, while his staff was apprehensive about shifting some IT functions to the cloud, the value of the cloud computing is that it affords him the chance to “let someone in the cloud run e-mail and free up my guys’ time to work on stuff that does make a difference” (quoted in D’Auria and Nash, 2009). One of the profound issues that will need to be dealt with is the reluctance of both IT staff and users to switch to online applications. For instance, while there are free online options for both word processing and spreadsheet applications (i.e., Google Apps and Open Office), such systems have not proven to be 100 percent compatible with existing Microsoft Word and Excel files in terms of formatting, style, and templates. Thus, working with cloud options for such productivity software entails more work for users and IT than existing “shrink-wrapped” software options (Dignan, 2008).

Recent estimates are that, for every \$1 organizations spend on PCs in the enterprise, another \$8 is required for administrative support, maintenance, and upgrades (Miller, I. 2009). For the federal government, the equation may be higher—much higher. In fact, infrastructure costs have been estimated to consume *almost half* of the federal IT budget today.

Thus, rapidly increasing maintenance costs for legacy systems may be one of the prime forces that will drive adoption of cloud computing. Radha Sekhar, assistant deputy undersecretary of defense comptroller for financial management, described the shift to a greater use of cloud computing as “inevitable,” stating, “These are investments the government has to make, otherwise the costs of computing will be very high. There are no limits, especially in the defense budget. If we don’t have innovative, smart technical solutions, the budget will keep growing” (quoted in Nagesh, 2009b).

Certainly, the nature of IT jobs and the skills required to perform them will change markedly over the next decade. There will be less manual work needed, both in data centers (“racking and stacking”) and in the field (doing installations and upgrades). At the same time, there will be a greater emphasis on the negotiation, conceptual, and people skills needed to manage contracted cloud services. Indeed, in the near future, there will be a great need for developing expertise in specifying, negotiating, and managing service-level and organizational agreements (Robinson, 2009b). All of this will lead to IT executives being able to focus on how best to deliver services, rather than where they are hosted or how they are implemented (Schurr, 2008). This will, of necessity, lead to changes in how IT and IT managers are evaluated for their performance.

How will this impact IT employment overall? Erlanger (2009) offered a very informative, long-term assessment on the impact of cloud computing on IT jobs and the IT workforce. He noted that, while cloud computing will create jobs in the near term, over the next decade, there will be a significant displacement of many of the “nuts and bolts” technology jobs in IT—doing “hands-on” work in maintenance, upgrades, and the like. Overall, the technical skills needed for IT jobs will likely decrease, as many jobs in the field become more administrative in nature (overseeing and negotiating contracts, handling customer inquiries, and the like). Some have referred to this as a shift away from “blue-collar” IT jobs and careers toward a more white-collar IT workforce.

Golden (2009e) has offered the reminder that, while IT has seen platform transitions before—from mainframe to Windows to the web, the fact is that

“human capital is the most difficult kind to upgrade.” Thus, at a time when cloud computing is emerging so quickly, it will be difficult to train IT professionals on cloud technologies—and then to retain them. As Erlanger (2009) pointed out, this will require retraining of many present IT workers—and those jobs that are found with cloud providers will indeed be away from “traditional” tech centers and major cities and in the rural, power-friendly areas where major cloud data centers will tend to be more commonly located.

## Challenge Nine: The Need to Assess the Return on Investment of Cloud Computing

What—and when—will be the return on investment (ROI) of cloud computing? Most analysts have projected that cloud computing can deliver cost savings by outsourcing IT operations—perhaps as much as three to five times more cheaply than in-house data centers and hosted applications (Greenberg, 2009b). Based on anecdotal evidence from government entities, the ROI of cloud computing initiatives—from cloud storage and e-mail to SaaS applications—can be significant, as costs savings have been demonstrated by using hosted applications and having less need for internal IT resources and staffing (Hall, 2009e). However, a report from McKinsey & Company has called this into question. McKinsey found that cloud computing could actually be more expensive than in-house IT operations, especially if organizations look to adopt best practices to improve their internal server utilization rates through a combination of virtualization and reduced capacity (O’Gara, 2009b).

The ROI calculation is a bit different for the public sector than for private sector companies, specifically due to the tax treatment of capital costs. Private sector firms can write off the cost of capital investments on their taxes as a depreciation expense. Thus, they may find the concept of funding their IT needs as a variable expense, rather than a fixed cost, less attractive for tax reasons. However, for government IT leaders, a cost is a cost, so with no concern over depreciation of equipment, cloud computing may in fact be more attractive to public sector executives than to their for-profit brethren (Chabrow, 2009c).

However, in other areas, there are no differences in costing between government and for-profit organiza-

tions. First, the shift to cloud computing will not be without a cost. To the contrary, even if shifting to free resources, there will be switching costs involved. Patrick Stingley spoke of the retooling and migration costs that will be incurred in the switch, stating, “It will cost money to move to the cloud; this isn’t going to be free” (quoted in Erlichman, 2009).

Stingley believes that one of the objectives of cloud computing should be to prepare agencies for making their data portable—to separate the data from the proprietary systems it is run on: “Because we will need to be able to move from Provider A to Provider B, this will force us to move to open data” (quoted in Jackson, 2009d). There are certainly indirect costs that will apply to IT operations regardless of how much of the operations are shifted to cloud computing. For instance, in the accounts payable area, there still will be the processing and payment of invoices, whether they are buying servers and software or paying for cloud storage or applications (Golden, 2009f). Finally, the reality is that any organization—public or private—that moves a core function to cloud computing will likely face having to run a hybrid solution for some time to come—not a hybrid cloud, but a dual track of the old, in-house system and the new, cloud-based solution (Hodgin, 2009).

An organization’s cloud computing strategy should thus certainly not be an “all or nothing” gambit, with a sudden “we’re in” or “we’re staying out of it” decision. Instead, a cloud strategy should look to create “a portfolio of cloud resources,” combining public, private, and hybrid cloud elements with the organization’s legacy systems and resources (Staten, 2009). Laurence Millar, former CIO of the Government of New Zealand, recently framed the cost-versus-control trade-off between private and public clouds in a very astute manner, commenting, “A private government cloud is all very well, and at the moment it is probably worth paying a price premium for the control and security that it supposedly provides. But it is a risk-versus-cost equation. A private cloud will half the cost of computing. But the public cloud will half that cost again” (quoted in Hicks, 2009a).

Many observers believe that what will emerge are hybrid models, whereby organizations will combine the use of their own private in-house clouds for running mission-critical operations and hosting sensitive data with the use of public clouds for

routine work, operations, and storage. The key will be to develop decision rules to determine which applications and data should remain in-house and which are candidates for the cloud.

Finally, Golden (2009f) argues that the most significant cost of not shifting to greater utilization of cloud computing is in the time and attention of senior IT and organizational leadership. As he framed the issue, “Every minute spent on reviewing an RFP for procuring another tranche of servers is a minute not devoted to how to use IT for competitive business advantage.” Yet, one challenge facing cloud adoption is the simple fact that, as organizations choose to move some of their data and applications to the cloud, rather than running a 100 percent internal IT operation, this will necessitate the development of a second management front—and additional time, training, and managerial attention—to managing cloud operations.

## Challenge Ten: The Need for Government Cloud Coordination

As federal agencies establish their own private cloud environments, analysts have forecast that we are likely to see agencies sharing data centers and cloud services to facilitate collaboration and to share costs (Haynie, 2009). Some have even forecast that we may well see an “über-cloud” emerge, where, across the federal government, there can be a sharing of data and applications (Foley, 2009a). It is vital that cloud adoption be government-wide, and not done on a piecemeal basis, in order not just to prevent more information silos from developing, but to provide the scale that will make the concept work even better than in an agency-by-agency framework. As the NBC’s Doug Bourgeois commented, “Without scale and a lot of it, this is not going to be economical” (quoted in Nagesh, 2009b). In fact, some have predicted that “the federal government could run the biggest cloud ever” (Gross, 2009c).

Stingley stated his belief that it is important for the federal government to have a well-coordinated cloud computing strategy, noting, “We need to do this as a government, not as a whole bunch of little armed camps” (quoted in Erlichman, 2009). Given that the scale economies and need to eliminate redundancies will push for a “one cloud” solution, the GSA would appear to be the reasonable home for a federal cloud; as a central service provider for

the entire government, it could host computing capacity tomorrow as it does office space and vehicles today (Hoover, 2009h).

Thus, the Kundra-backed “GSA storefront” concept, Apps.gov, may indeed be the best prescription for pursuing cloud computing on the federal level. Likewise, we may see statewide or even multistate consortia develop in the U.S. for cloud computing (maybe hybrid clouds for multiple governments hosted on the same, physically and cyberprotected grounds), and abroad. It will be vital to see national cloud computing strategies take form, with their own champions for the cause.

We have seen predictions that, due to the cost and operational benefits of cloud computing, more and more companies will find themselves outsourcing most—if not all—of their IT to cloud providers, creating what Appirio, Inc. (2008) termed “serverless” companies. And this will not be true just for small enterprises, as it has been predicted that organizations of all sizes will find it beneficial to concentrate on and optimize their business processes by outsourcing the IT function. So, why not “serverless government”? Perhaps not outsourcing all of IT and all data storage/handling—that may be impossible for a governmental body, however, particularly for cities, counties, colleges and universities, and even perhaps state agencies, this may be a viable proposition, particularly as cloud offerings expand and are made more secure and reliable.

Finally, Doctorow (2009) recently criticized IT leaders in a Harvard Business School publication, observing that “the dirty secret of corporate IT is that its primary mission is to serve yesterday’s technology needs, even if that means strangling tomorrow’s technology solutions.” In the public sector, too often we speak in terms of not just dealing with “information silos,” but with a legacy of outdated systems that run in programming that is cumbersome and difficult to work with. The prime example of this is found in the federal government, in the fact that many agencies still rely on Cobol for critical applications. As Haynie (2009) discussed at length, cloud computing can further the application modernization movement under way to help move federal agencies away from the “Cobol world” in a fraction of the time and at a far lower cost than rewriting or replacing these critical applications.