Cloud computing by government agencies
Meeting the business and security challenges in the cloud

Skill Level: Intermediate

Shahid N Shah (shahid.shah@netspective.com)
CEO and Chief Architect
Netspective Communications, LLC

17 Aug 2010

The United States federal government has the largest annual IT budget of any organization, almost $80 billion in 2010 alone. To save money and improve services, the government is beginning to adopt a cloud first approach towards procuring new and replacement systems. The business cases and technical benefits for moving into the cloud are the same for the government as they are for other firms, only the savings and challenges are much bigger. Government agencies have two special challenges: procurement and security. This article briefly describes the procurement challenges and then jumps into advising government cloud service purchasers on the positives and negatives of security in the cloud, and how to manage their potential vendors' security risks. The security threats are covered from the government's point of view, but smart cloud vendors will take it as a preview of what questions the government might ask them and prepare accordingly.

Business and technical challenges of moving to the cloud

The Obama Administration has been particularly focused on using modern Web 2.0 and cloud computing technologies to help improve government services. That request was actually written into the budgets for the next few years, which means that, officially and by law, all agencies are supposed to be thinking cloud first now. Due to this cloud-first thinking, an impressive data center consolidation analysis effort is underway and the Administration is looking for ways to accelerate cloud adoption. Of course, any big move to cloud computing by the government is a multiyear initiative, but it's clear that the top IT leadership in government is ready to
The business cases and technical benefits for moving into the cloud are the same for the government as they are for other firms, only the challenges and potential savings are much larger. If the government can reduce even five percent of its costs over the next few years, it will mean billions of dollars of savings; so it’s easy to understand why senior IT leaders in the government are thinking about the cloud.

Most of the typical cloud business challenges are the same as in other environments, but the government has a few special challenges. The first is procurement. How do you buy on-demand cloud services if the government does its budgeting years in advance when the demand for something is not known? The contracting and procurement processes are typically lengthy and arduous because the government tries to negotiate fewer contracts that fit all agencies' needs and for the long-term. Because they are long-term contracts, they are easily outpaced by the technology innovation cycle, meaning the government ends up buying older, more expensive servers, networks, data centers, and so on.

While the procurement and cultural buying barriers are substantial, the second most important barrier, which is also the case in commercial firms but with bigger and farther reaching implications for the government, is security in the cloud. Security rules that the government must adhere to are usually written by Congress as formal regulations with the force of law; they are far more stringent and less forgiving than those in the commercial sector.

Overall security advantages gained by moving to the cloud

Many government agencies host their public data (unprotected data they share with citizens) in the same networks (logically speaking) as their private data. By shifting public data to an external cloud, agencies can reduce the exposure of internal sensitive data because the public and private servers don't sit near each other.

Today, each agency has its own network and literally spends billions of dollars to architect, build, document, secure, monitor, and audit hundreds of different networks that probably do similar things. By moving into the cloud, security auditing and testing and the related tasks are simpler because the infrastructures and networks look alike or are identical.

Redundancy and disaster recovery (DR) or continuity of operations (COOP) is very expensive given the current structure of applications, platforms, and networks in most agencies. By moving into the cloud and more importantly into virtualization technologies, you can see easier DR and COOP strategies because the cloud offers easier backups and better redundancy.

It’s easy to see how DR and COOP are easier—all reputable cloud vendors have
multiple redundant data centers and offer virtual machine replication across multiple sites. What’s easy to overlook is the easier backup offerings—many vendors offer storage area networks (SANs) for data redundancy across multiple disk drives, meaning you’ll get real-time backups. In addition, though, vendors also offer snapshots for regular backups of entire disks that you can roll back to and ultimately move to tape or offsite storage if you purchase that service. The DR, COOP, and backup offerings are not just technical features, they are important security considerations because loss of data and data leakage often occurs due to poor DR and backup strategies.

Overall security challenges presented by moving to the cloud

While some benefits are associated with moving into the cloud, most IT professionals see many reasons to be afraid. Here are common questions that security professionals ask:

• How do I know I can trust your (the vendor’s) security model? Will your documentation and process be transparent? How do I know that you’re probably responding to audit findings?

• Can your proprietary implementation be easily examined to uncover faults? Will you support my intrusion and criminal investigations in the same way that I can do within my network today?

• Do you support Trusted Internet Connections (TICs) with full auditing for Internet traffic bandwidth utilized by the government? TICs are being mandated and most cloud providers don’t even know what TIC is.

• How do you track classified data leaks into unclassified systems? If there’s ever a case of classified information accidentally “leaking” into an unclassified system, the government can come to your facility and request that you wipe entire hard drives to clean up after such an information leak. What kinds of processes do you have in place to deal with a hard drive wipe in case you shared data for multiple customers on a single hard drive? How do you satisfy concerns around liability of mixing classified and unclassified data?

• How do you guarantee that government data stays on servers physically located within the continental United States? There are stringent rules written by Congress and regulations enacted by different presidential administrations that require this to be the case.

• Are backups outside of your system boundary? Is the transport over a secure connection and encrypted at a remote location? Is it encrypted during transit offsite? What is the physical security and technical security controls at the offsite location? Are the backups sent to foreign locations
for offsite storage? Does the backup site have the same security controls as the primary site?

Most of these questions—multi-tenancy, encryption, and compliance concerns—boil down to trust. There are more questions than can easily be answered by most cloud vendors. If you're a cloud vendor looking to serve the government or you're a government buyer wondering what technical security questions to focus on, here are some pointers. This article covers the security threats from the government's point of view, but smart cloud vendors will take it as a preview of what questions the government might ask them and prepare accordingly.

Next, you'll take a look at specific security challenges for government cloud users.

Personnel, identity management, and access control risks

You want to be aware of threats including malicious insiders, such as the person or people responsible for recently leaking over 90,000 pages of classified documents concerning the war in Afghanistan. Proper identity management and access control are difficult already within the boundaries of a single entity's IT system. But when a system crosses boundaries, with part of it being within an internal network and a smaller or larger part being in the cloud within another vendor's environment, it becomes even more difficult. If you help secure such hybrid systems, be sure to consider hiring practices at your cloud vendors. They should have at least as stringent hiring policies as your own. How will the vendor notify you when individuals that work on your data or systems come and leave? And, under what circumstances has someone left? If you can't trust the people at the vendor, you can't trust the vendor. For example, when an employee of your cloud vendor leaves, are you notified?

Once you're sure you know the hiring process and system provisioning rules, you'll want to understand their logical access and access privilege escalation process. Who decides the access rules and how are you notified when the access rules change? People are often most concerned with granting initial access. Remember though, that the more likely breaches occur when access is escalated for existing employees within a vendor but you're not notified of such escalation on your side (so that you can monitor usage differently). Identity and access monitoring for your own employees at the government are crucial, but you have other safeguards such as on-premise physical security to get to your network or VPNs for remote access that require two-factor authentication. From a security point of view, your cloud vendor's employees are just like your own employees, and, if the cloud vendor's employees are not following the same rules as your internal employees, you should count on a breach sooner or later.

For specific remediation of these kinds of risks, you might want to create key personnel lists at your cloud providers that are known and tracked by contractual
obligations. Conducting regular audits of information access is another common technique. You should require compliance reporting and monitoring tools be put in place that make the cloud vendor's processes completely transparent to the government staff overseeing the contract. The obvious things like requiring two-factor security and preventing sharing of credentials are important, but it's the intangibles and seeing whether security is in the DNA of the cloud vendor versus just something they see as a compliance effort that is even more important to ascertain.

Reputable vendors like IBM®, Amazon, Google, Microsoft®, and other household names already know how to do this kind of security work; the worry is for the software-focused Software as a Service (SaaS) or Platform as a Service (PaaS) vendors that have more application focus than system focus. If a cloud company is more consumer-focused than government-focused (or enterprise-focused) they will need more scrutiny because they don't deal as much with mission-critical data that can cause irreparable harm to the government.

Data leakage risks

Many kinds of intellectual property need to be protected, but data is arguably the most important: When you think of security you're not as concerned about people stealing your servers or applications. What you're really worried about, especially in the government, is the data that is stored on the servers. Data breaches cause data loss, also known as data leakage in those cases where the original data is preserved but copied from the sources. Numerous things can cause data security breaches:

- Altering data without the data owner's knowledge
- Deleting data in some unrecoverable way
- Obtaining data in nefarious ways and using it to cause harm to the government or its citizens

You know about the national security implications already: Classified data leaks can put soldiers in harm's way. However, commercial hacking and data breaches are even more common and need to be prevented. Here is a simple example: A contractor who works for the government might steal or borrow procurement-sensitive data for another contractor looking to benefit from insider information. This type of data leakage is easier to track when all the data and the users are within the same network; however, it's very difficult to track when the data and IT systems are out of your control in the cloud.

To help remediate the risk of data leakage, make sure you have contractually obligated your cloud vendor to maintain access logs and conduct regular audits of major systems like database servers [physical or virtual machine (VM)] and database systems (MySQL, ORACLE, DB2®, and so on). You need to know, for
example, what data is regularly reviewed and managed by your cloud vendor’s DBA team. If a cloud provider doesn’t already track this information and is doing something special for you, you may have a problem.

Cloud security is an emergent property of the entire system as well as a functional requirement. Treating security as a specific functional requirement is a start—systems that you buy and vendors that you choose need to be “secure” for sure. However, in most complex systems security must be understood as somewhat of an emergent property, meaning that you can actually have major parts of your system functionally secure, but the entire system might remain insecure and high risk. For example, your cloud vendor could have data encrypted at rest on their hard drives (secure) and your data might be transferred between sites in an encrypted fashion (also secure), but the users can write down their passwords or store them in their mobile phones (insecure). Many security professionals, and especially executive sponsors, often spend more time on technical security of components rather than the human factors that tie those components together—by doing so, risks are easily missed. This is even truer when going into the cloud where there are completely different organizations involved. If you treat security and its associated risks as an emergent property (something that “arises” from your system rather than is contained within it), you will able to better manage cloud security threats.

Another remediation effort surrounds data disposal. Some of the most common data leakage occurs not while the data is actively protected by DBAs but when hard drives are disposed, backup tapes are transferred from one environment to another, or media is scheduled for reuse. If you’re responsible for tracking data security at your cloud vendor, ask them about their data disposal plan and audit them carefully.

Multi-tenant hosting risks

Once you look at the broad attack vectors like access controls for personnel and data disposal, focus on the multi-tenancy and intermixing of data between different clients and how that data is protected. For example, an Infrastructure as a Service (IaaS) provider might offer five clients partitioned VM access to the same physical server. Accessing data in one VM from another protected VM on the same box is possible but very difficult. However, protecting a multi-tenant application from data leakage between clients is harder and leakage becomes more likely. You’ll want to ask your cloud vendor how they store multi-tenant data and if it’s possible for one tenant (you) to accidentally or maliciously access another tenant’s data. Most vendors and programmers will tell you that they have programmed safeguards, but a simple bug in access logic within an HTML or JavaScript file can spill large amounts of data. Multi-tenant systems that store everything in one logical and physical database are more prone to this kind of error than those that store each tenant’s data in separate logical databases with different schemas for each customer. Work closely with your vendors to figure out your data leakage risk. It is probably much higher than they think.
Handling secret information

Data encryption and translucent database techniques are two other common methods for handling secret information. Your vendors can choose full disk encryption, partial disk file system-based encryption, schema-based encryption, table encryption, column encryption, or a mix. FIPS 140-2 encryption should be a minimal requirement when appropriate for the specific data being protected (see Resources for a link to the "Federal Information Processing Standards publication 140-2"). The best thing to do is to ensure full-disk encryption unless your vendor really understands how to do the other types. However, even when your cloud vendor tells you that data is encrypted at rest in their database, ask them about their key management approach. Who holds the keys and how is key management done? If key management isn't secure and properly managed, the encryption is pointless. Some vendors will encrypt their disks yet put keys to the decryption on the same server because they don't understand the risks. Protecting government data is far more difficult than protecting commercial data so it's imperative that the vendor's personnel understand this. If you're using IaaS, you can control the encryption and key management to whatever degree you'd like. If, however, you're using PaaS or SaaS, you're more at the mercy of the cloud vendors so you'll want to be prescriptive in your requirements.

Also, keep in mind that while a vendor might have a Certification and Accreditation consultant (C&A) and say they are Federal Information Security Management Act (FISMA) compliant, it doesn't mean that your secret data is properly protected. As a government representative, you need to do further diligence to get the evidence you need to satisfy your executive sponsors.

Auditing and logging

Everyone, including the vendors, knows that auditing and logging is important. However, not everyone does it the right way: The system of record for logs should never be the same system as the system being logged; most operating systems include logs but those shouldn't be considered good enough. Remote syslog and real-time log shipping should be used in all circumstances, not just some. Application events, database logs, and security activity tracking should all be stored in a fully auditable centralized log with non-repudiation features such as hashing and guaranteed message delivery mechanisms. If a vendor has access to their own logs and can modify them, they aren't believable. The vendor should, of course, have access to their logs, but any log modifications should be impossible and their log management system should be able to detect tampering or hack attempts. When doing forensic analysis after an event, the logs are the primary evidentiary sources and they must be reliable and highly available.
Denial of service and defacing risks

Government systems are especially vulnerable to denial of service and defacing attacks where just embarrassing an agency, its mission, or its personnel is a goal unto itself. Packet flooding, also known as network bandwidth saturation, is the most common risk and you should ask your vendor how they specifically handle that because many cloud providers (especially SaaS) just assume it's handled by someone else. Also, you should inquire as to how they identify botnets and defend against malicious network traffic that is likely to make it into IaaS, PaaS, or SaaS environments. They should be performing deep packet inspection for network attacks with known signatures and automatically guard against flooding of large data packets that might crash web or application servers.

Spoofing, eavesdropping, and packet sniffing risks

If your government IaaS, PaaS, or SaaS requirements include knowing about sources of data through IP addresses or DNS, then you'll want to be sure your provider can guard against IP and DNS spoofing and ARP flooding. The vendors should also be contractually obligated to show how they prevent packet tampering, prevent enumeration of your private services by other tenants, and prevent tampering with your configuration data or encryption keys that might need extra protection.

Conclusion

You've learned that governments are large users of all kinds of IT systems. In an effort to be more agile, meet their mission goals faster, reduce development risks, and reduce overall budgets and costs associated with running IT systems, most government organizations are looking at implementing a cloud solution. The cloud has enormous business and some security benefits and over time it will be better understood and used more effectively. At this time, government staff should be careful because the cloud is new. Nobody, not even cloud vendors, are aware of all the security risks. But this shouldn't stop you from beginning to experiment with vendors who show they're serious about security and know their threat models well.
Resources

Learn

- **Federal Information Security Management Act (FISMA) implementation project**: Learn to promote the development of key security standards and guidelines to support the implementation of and compliance.

- **Federal Information Processing Standards publication 140-2**: Learn more about security requirements for cryptographic modules.

- **Navigate the cloud computing labyrinth** (Brett McLaughlin, developerWorks, March 2009): Make an educated decision about the best cloud computing platform for your particular application requirements.

- **IBM Cloud Computing**: Learn all about IBM’s vision for cloud computing.

- **Cloud Computing**: Read this Wikipedia article to learn about SaaS, IaaS, and PaaS.


- **Cloud Computing Tutorial** (Jens Nimis, SlideShare, July 2009): Check out this introduction to the world of cloud computing.

- **Industries zone on developerWorks**: Get all the latest industry-specific technical resources for developers.

- **IBM developerWorks Cloud Computing Zone**: Find updated resources on cloud computing.

- **Industries library**: See the developerWorks Industries library for technical articles and tips, tutorials, standards, and IBM Redbooks.

- **My developerWorks**: Personalize your developerWorks experience.

- **developerWorks technical events and webcasts**: Stay current with technology in these sessions.

- **developerWorks on Twitter**: Join today to follow developerWorks tweets.

- **developerWorks podcasts**: Listen to interesting interviews and discussions for software developers.

Get products and technologies

- The **IBM Smart Business Development and Test on the IBM Cloud**: Start developing your applications for the cloud.

- **IBM product evaluation versions**: Download or explore the online trials in the
IBM SOA Sandbox and get your hands on application development tools and middleware products from DB2®, Lotus®, Rational®, Tivoli®, and WebSphere®.

Discuss

- developerWorks blogs: Check out these blogs and get involved.

About the author

Shahid N Shah

Shahid N. Shah is an internationally recognized and influential IT thought leader with almost 20 years of architecture and development experience including 10 years of senior public sector, non-profit, and healthcare technology strategy specialties. He is a consultant to various federal agencies on general IT as well cloud-specific strategies and won Federal Computer Week's coveted "Fed 100" award given to IT experts that have made a big impact in the government. Shahid has consulted, architected, and built multiple public and protected complex government systems at the Executive Office of the President, NIH, VA, and OMB. His technology expertise includes citizen-centric government strategy, service-oriented and event-driven architectures, Java/JEE, .NET, agile development, data integration, and legacy modernization.