Survivability and Information Assurance in the Cloud

Melvin B. Greer
Chief Strategist, Cloud Computing
Lockheed Martin
(301) 921 7028
melvin.greer@lmco.com

Abstract
The threat landscape facing the Federal Government is growing, from underground cybercrime economy and burgeoning malware production to rumors of cyber war. Business leaders and security professionals focused on this threat landscape and evaluating cloud computing advantages also need to address cloud computing’s unique survivability and information assurance risks.

Keywords
Cloud Computing, Security, Information Assurance

Introduction
In the past year cloud computing has moved from hype to being a compelling net-centric approach behind Federal government information technology. Although its merits are yet to be fully realized, this new approach promises speed, agility and low cost with greatly improved security, privacy and confidentiality. The Federal Cloud Computing Initiative from the Office of Management and Budget is focused on:

– migration towards a services-based environment that is technology and vendor-agnostic
– rapid deployment of technology solutions for the Federal government
– scalability for existing and new capabilities
– savings through virtualization
– reduction of infrastructure, buildings, power, and staffing cost
– improve government’s ability to create a transparent, open and participatory government

Government leaders looking to evaluate and mitigate the risks of adopting cloud computing technologies find important benefits and some survivability and information assurance challenges not to be ignored. This paper identifies six critical risks and the need for a Federal Cloud Information Assurance Baseline that could establish the cloud risk mitigating criteria necessary for broad cloud adoption. Examining cloud computing
advantages and also addressing its unique survivability and information assurance risks will make cloud computing more relevant to the Federal Government.

**Survivability and Information Assurance Risks**

The threat landscape facing the Federal Government is growing, from underground cybercrime economy and burgeoning malware production to rumors of cyber war. Business leaders and security professionals who are focused on this threat landscape and are evaluating cloud computing have identified six critical risks that impact cloud adoption in the Federal Government.

**Risk-Testing Risk**

It is not easy to determine if a cloud service provider is mitigating key risks. Testing is difficult to arrange and conduct (you have to visit the provider's facilities), and often is not really offered by the provider. If there is not enough information to determine just how well a provider is managing risk, then the only prudent (and defensible) conclusion is that it is not.

**Data Location Risk**

It is hard to know where data is being stored. The question may be which disk farm, which data center or even which country. The Federal government has policies or laws that require some level of control over this. The Federal government is required by law to keep data on servers in their own country. The International Traffic in Arms Regulations (ITAR) prevents some firms from storing product data outside the country and the USA Patriot Act may allow the U.S. government access to any information stored within its borders. In the European Union, privacy laws have established in-country restrictions on person-related data. There may be other related risks, including disclosure when data crosses borders.

**Data and Code Portability Risk**

Once data has been put into a cloud environment, particularly a full application system offered as a cloud service or Software as a Service (SaaS), it can be difficult to get the data back out. Beyond the data, it may be hard to get process (and the code that executes that process) out of the provider.

**Data Loss Risk**

Any cloud environment and any cloud provider can lose data. Cloud providers may be better or worse than an internal information technology organization regarding this issue — but given the low maturity and simple age of cloud service offerings (Amazon S3, an original entrant in this market, just celebrated its third birthday), it is prudent to assume
the worst. There have been some disturbing — albeit isolated — cases of providers either suffering a complete technical meltdown or going out of business. Both forms of failure have resulted in non recoverable data losses. Many cloud services do not come with backup/restore capability included — it may have to be added as an option.

**Data Security (Privacy) Risk**

Agencies data is considered less secure and more prone to cyber attack when it is stored externally rather than internally. Agency data may be more vulnerable to being accessed, copied or compromised. Of course, most agencies underestimate the results of their internal data security, so internal security is not without risk. Still, storing data externally could be worse.

**Vendor Viability Risk**

The cloud provider may fail and completely go out of business. This may not happen to an Amazon, Google or salesforce.com, but the economic downturn may prove fatal to the viability of smaller vendors. Remember, this happened back in the external service provider days of the Internet bubble, too. Even large vendors might decide to stop offering a particular cloud computing service. Note also that the “cloud” of providers may hide some viability risk, as some service providers may leverage others that in turn could go out of business.

There are many other risks inherent in cloud computing service provisioning. This represents a current list of the top inhibitors. Over time, the Federal government perceptions may change and other risks will become greater inhibitors to adoption.

None of the risks discussed here is a "showstopper“ for all agencies and for all specific use cases within the Federal government, but they will be for some. It is important to confirm that these inhibitors are understood and reasonably mitigated to get stakeholder approval for investments in cloud computing services.

Alleviating these risks will require detailed mitigation strategies along with people and process changes. Certain IT and business roles will be needed to define appropriate risk mitigation plans. In planning teams, it is critical to include subject matter experts, and to address information assurance, security and risk. In particular, defining specific criteria designed to:

- Assess the risk of using cloud versus on-premise environment
- Compare different cloud provider offers and terms of service
- Obtain assurance from selected cloud providers focused on effectively securing cloud-specific architectures
- Provide a clear set of information assurance and security requirements for cloud providers
These criteria and other important survivability and information assurance capabilities are an important addition to the Federal Cloud Computing Initiative and should provide minimum baseline criteria for any agency investigating the use of cloud computing. This paper proposes a Federal Government Cloud Information Assurance Baseline (CIAB) useful in accelerating the adoption of cloud computing, and assisting the government in realizing cloud computing target benefits.

**Cloud Information Assurance Baseline**

Organizations considering cloud-based services must understand the associated risks and define acceptable use cases and necessary compensating controls before allowing cloud services to be used for regulated or sensitive information. Cloud computing environments have information technology risks in common with any externally provided service. There are also some unique attributes that require risk assessment in areas such as data integrity, recovery and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance and auditing. Key areas agencies should baseline include:

- Privileged User Access
- Compliance
- Data Location
- Data Segregation
- Availability
- Recovery
- Investigative Support
- Viability
- Support in Reducing Risk

**Privileged User Access**

When sensitive data is processed outside the enterprise, or by non-employees, it means that organizational managers are less immediately aware of the nature and level of risk, and that they have no direct ability to control these risks. Any externally sourced IT service bypasses the physical, logical and personnel controls that IT normally provides for in-house applications. Although it is certainly the case that trusted company employees can make mistakes and commit fraud, and it is not the case that outsiders are automatically less ethical than employees, experienced security specialists are highly aware of the inverse relationship between loyalty and risk. It is only prudent to put a higher level of trust in your fellow employees than in people who do not have a long-term commitment to your organization. Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access.

**Compliance**

Cloud service providers may be new, but most regulations hold the user of the service ultimately responsible for the security and integrity of their corporate and customer data, even when it is held by the service provider. Traditional service providers submit to external audits and security certifications, providing their customers with information on
the specific controls that were evaluated. A cloud computing provider that is unwilling or unable to do this is signaling that customers can only use them for the most trivial functions.

Data Location
A unique ramification of the cloud computing model is that you probably cannot know where your data is hosted. Indeed, in an increasingly globalized infrastructure, you might not even know in which country your data is stored, which should be of concern to anyone needing to meet national privacy regulations. Will providers commit to storing and processing data in specific jurisdictions?

Data Segregation
Virtually all cloud offerings use Secure Sockets Layer to protect data in transit, but most cloud offerings store data in a shared environment. Find out what is done to segregate data at rest. If your data can be read at your provider's site, then you have to assume that it will be read. Increasingly, Software-as-a-Service (SaaS) vendors are touting the use of encryption for the stored data. Encryption is an important tool in the prevention unauthorized access to data, but it is not a panacea. While key length and choice of encryption algorithm are important elements to verify, the most likely failure mode is through an implementation mistake that results in unexpected and exploitable weaknesses. Ask for evidence that the encryption implementation was designed and tested by experienced specialists. Find out who performed the protocol analysis and code reviews. Encryption accidents can make data totally unusable, and even normal encryption can complicate availability. If your data will be stored and backed up in encrypted form, then find out who has access to the decryption keys and whether it is possible for authorized individuals at your company to gain access to their employees' data in an emergency.

Availability
Reliability is one of the core advantages inherent in the cloud computing model. By its very nature, it is highly scalable, capable of meeting wide variations in processing requirements and insulating users from site problems. However, many cloud-based offerings do not provide service-level commitments that are typically needed for critical business processes. Organizations should define service-level requirements for any nontrivial information technology workload and demand service-level agreements from the provider (internal information technology, traditional outsourcer, cloud computing provider) and ensure that the contract contains penalty clauses when service-level agreements are not met.

Recovery
Beyond continuity of operations, organizations need to know how cloud offerings will recover from total disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure. Even if an cloud provider refuses to tell you exactly where it will store your data, it should be able to tell
Survivability and Information Assurance in the Cloud

you what would happen to your data and service if one of its sites succumbs to a disaster. Does it have the ability to do a complete restoration, and how long will it take?

Investigative Support
Internal investigations of inappropriate or illegal activity and electronic discovery are difficult and expensive propositions, even when conducted in your infrastructure. If you are considering purchasing a service that would process anything considered a business record, or if you otherwise anticipate a need to conduct investigations, then you cannot assume that a service provider will be willing, or even able, to support them. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then the only safe assumption is that investigation and discovery requests will be impossible.

Viability
The long-term viability of any external service provider is also something that needs to be evaluated. What would happen to your service if the provider goes broke or is acquired? What assurance can it offer that this will not happen, or if it does, that you will be able to use your data? Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application?

Support in Reducing Risk
Evaluate the information and support provided to enable customer staff to understand how to safely and reliably use their product. Are instructions provided to administrators and managers for setting and monitoring policies? Are users provided with instructions on how to avoid phishing or malware attacks?

This Federal Government Cloud Information Assurance Baseline should be used along with the Federal Cloud Initiative to ensure agencies achieve survivability and information assurance targets consistent with use of all classes of government data.

**Critical Success Factors and Recommendations**

The following critical success factors and recommendations should guide any Federal Government agencies investigating the use of cloud computing technologies.

Critical Success Factors

- The most practical way to evaluate the risks associated with using a service in the cloud is to get a third party to do it.
- Cloud computing information technology risks in areas such as data segregation, data privacy, privileged user access, service provider viability, availability and recovery should be assessed like any other externally provided service.
Survivability and Information Assurance in the Cloud

- Location independence and the possibility of service provider "subcontracting" result in information technology risks, legal issues and compliance issues that are unique to cloud computing.
- If agencies are making unauthorized use of external computing services, then they are circumventing security policies and creating unrecognized and unmanaged information-related risks.

Recommendations

- Agencies that have information technology risk assessment capabilities and controls for externally sourced services should apply them to the appropriate aspects of cloud computing.
- Legal, regulatory and audit issues associated with location independence and service subcontracting should be assessed before cloud-based services are used.
- Demand transparency. Think seriously before contracting for information technology services with a cloud provider that refuses to provide detailed information on its security and continuity management programs.
- Develop a strategy for the controlled and secure use of alternative delivery mechanisms, so that agencies know when they are appropriate to use and have a recognized approval process to follow.

References
