Survivability and Information Assurance in the Cloud

Melvin Greer
Chief Strategist, Cloud Computing
Lockheed Martin
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.

1. 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 an increased focus on 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
- improving government's ability to create a transparent, open and participatory government

Government leaders looking to evaluate and mitigate the risks of adopting secure 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.

2. Survivability and Information Assurance Risks

Online threats to the world's critical infrastructure continue to grow, according to "In the Crossfire: Critical Infrastructure in the Age of Cyber War," a Center for Strategic and International Studies (CSIS) report. The report is based on detailed surveys of 600 security professionals in 14 countries and was touted as the most complete to date of the security posture of the global critical infrastructure. The report finds that 60 percent of those interviewed had experienced theft-of-service attacks and nearly 90 percent were infected by viruses or other malicious code. But victimization rates were also over seventy percent for a wide range of other attacks, including low-level DDOS and vandalism, insider or employee threats, loss or leakage of sensitive data, and phishing or pharming. Defenses mounted against these threats appeared to be inadequate. 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. These risks are 1) Risk Testing, 2) Data Location, 3) Data and Code Portability, 4) Data Loss, 5) Data Security (Privacy), and 6) Vendor Viability.

3. Risk Mitigation

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.

4. 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. The baseline would be governed by the current Federal Cloud Computing Initiative cross agency organization and include the following key areas: Privileged User Access, Compliance, Data Location, Data Segregation, Availability, Recovery, Investigative Support, Viability, Support in Reducing Risk.

5. Success Factors and Recommendations

Alleviating these risks areas will require the detailed mitigation strategies along with people and process changes. Certain IT and business roles will be needed to define appropriate risk mitigation plans. It is critical to include application development and security subject matter experts, and to address information assurance, security and risk. 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.
- 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.

6. References

[1] Office of Management & Budget, General Services Administration, Federal CIO Council, Industry Advisory Council, "Federal Cloud Initiative", 2009.

[2] Melvin Greer, "Software as a Service Inflection Point: Using Cloud Computing to Deliver Business Agility", iUniverse, 2009.

[3] Center for Strategic and International Studies (CSIS), "In the Crossfire: Critical Infrastructure in the Age of Cyber War", 2010.