B28 Acquisition Issues With Cloud Computing

Ernesto F. Rojas, MBA, PO Box 597, Seabrook, TX 77586*

After attending this presentation, attendees will be able to understand the principal issues that exist in operating in a public cloud computing environment. Examples of problems with multiple providers, data recovery, electronic discovery document collection, and other areas of interest will be addressed while contrast and comparison to traditional computing environments will also be discussed.

This presentation will impact the forensic science community by addressing issues related to the acquisition and migration to cloud computing environments by commercial and government entities and how they affect regulatory and legal requirements.

Cloud Computing has for the past two years become the latest must have of the ever-exploding computing innovation world.[1] Computing as a utility has many features that make the transition to the services extremely attractive by transferring capital requirements and technical responsibilities for operations along with other attractive features. In the process of rushing to order the latest cloud based software or service the user community is ignoring many important issues that will, once adopted, come to bear unforeseen problems at the worst possible moment. [2]

One of the principal issues in using cloud computing is the location of the data. A review of cloud computing service agreements show that the majority do not address the location of the data, leaving physical and jurisdictional locations to the decision of the cloud provider. This issue of location becomes important when there are legal requirements to keep certain type of information in conformance with regulatory and judicial regulations.[3]

Security is another major issue that in many cases goes unmentioned in cloud computing agreements; this is a major problem with Application-as-a-Service providers where the provider is asking the consumer to fully trust that the provider is handling all security issues to prevent theft and/or unauthorized manipulation of the users data.[4] Security in the cloud is rapidly becoming a world of specialists that provide security and authentication services to Cloud Service Providers (CSP) as a service, separating the operating and legal responsibilities and allowing for the transferring of risks to users in making sound choices in the selection of services.[5,6] In summary, this presentation raises issues that need to be considered before committing to a Cloud computing environment by a prospective user.

References:

1. Buckles, Greg; Cloud Providers and the Fog of War, eDJ Group blog post; Nov. 14, 2012, 9:10 AM.
2. Dykstra, Josiah, et al.; Acquiring Forensic Evidence from Infrastructure-as-a-Service; Cyber Defense Lab, Department of CSEE, University of Maryland, Baltimore County (UMBC); April 2012.
3. Taylor, Mark, et al.; Forensic Investigation of Cloud Computing Systems; Network Security; March 2011
4. Ruan, Keyun, et al.; Cloud forensics: An overview; Center for Cybercrime Investigation, University College Dublin, IBM Ireland;
5. Grimes, Roger; Staying Secure in the Cloud; InfoWorld.com Deep Dive Series;
6. Peter Hustinx, European Data Protection Supervisor; EDPS: responsibility in the Cloud should not be up in the air; EDPS; November 16, 2012.

Cloud, Business, Computing