Cloud Computing Technology's Biggest Problem: Where Is My Data?

Don Reese
Maricopa TekWorx

'The Cloud' is a term that dominates information technology these days, and unless you work in the field, you may not understand just what is meant by the term. This is one of the hottest topics in information technology today, and 'The Cloud' has not only taken the industry by storm, but continues to enable businesses to become more and more efficient. However, some major issues have arisen as cloud technologies have gained acceptance: data security, accessibility and availability. What happens if you or your customers are unable to access your cloud applications? What if the cloud provider's security is breached? Finally, what happens to your data if your cloud provider becomes unable to provide your service, or you wish to change providers? These are all pressing questions IT Managers and CIO's have to answer.

In the beginning of the computer era from the 1940's through the 1970's, computers were very big and very expensive; some were as big as rooms and cost several millions of dollars. This led to what they called 'time-share' systems, where companies who couldn't afford to spend millions of dollars on computers could instead rent computer time for hundreds or thousands of dollars, so you would have one big computer running computer programs for many different companies who had a terminal connected to these big mainframes over phone lines. This was originally accomplished by running each program sequentially for each client. As these 'mainframe' computers became more powerful and their operating systems became more sophisticated, techniques were devised to logically 'partition' the operating system, allowing multiple clients to run programs simultaneously without interfering with any other client. These 'logical partitions' (known as LPARS) are the direct forerunner of what has come to be known as 'Virtualization' (Dimitrios Zissis 3).

As the personal computer revolution took off, and computers continued to become more powerful, less expensive and able to fit on or underneath a desk, 'distributed computing' became the watchword of the industry, and empowered individual users to use database and spreadsheet programs (among others) to recreate the work that formerly had to be done on a mainframe computer at much higher cost. The explosion of the use of personal computers from the mid-1970's through the 1990's however created problems of a different sort for companies with large numbers of personal computer users, namely the increased energy costs required to run them, the increase in personnel costs required to manage and maintain them, and the increase in security risks due to so many people having access to corporate data.

'Virtualization' suddenly burst onto the scene to help solve all three of these issues, although the concept stemmed from decades earlier. As personal computers became more and more powerful, the software running on them needed less and less of the computers' resources, and so a method was devised to create what was now called a 'virtual machine' that would run within the operating system of a physical computer, sharing the resources but behaving as a totally separate computer. Virtualization software became increasingly sophisticated to where today a single (albeit well-appointed) computer can host dozens or hundreds of virtual machines (Dimitrios Zissis 3).

Virtualization technology, along with the increasing ubiquity of the Internet, emboldened people to start talking up this great new concept – 'Cloud Computing', which at its essence is virtualized servers in a data center running software and providing services, connected to over the Internet. Cloud Computing has been labeled as significant a development as the development of the national electrical grid: "When companies were freed from having to create their own electricity, they were able to focus on the core competencies of their line of business and the

needs of their customers. Likewise, cloud computing liberates IT organizations from having to devote precious people and budget to activities which don't directly contribute to their bottom line, while still enabling them to obtain the necessary infrastructure functionality to continue to run their businesses" (Amazon Web Services).

Today, there are many flavors of Cloud Computing, but generally the fall into one of three categories, Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS). SaaS is probably what most consumers are familiar with, whether or not they recognize the term. "The service delivered is the use of software at the supplier's remote site." (Bragonier 3) Some of the most popular SaaS products are Hotmail, Gmail and Google Maps. Platform-as-a-Service provides a more sophisticated and customizable environment to the user, often allowing you to modify the appearance of the user interface, but not the underlying computers or operating systems (Ibid). Some examples of PaaS include MySpace, Facebook, Blogger and many web hosting providers like GoDaddy and RackSpace. Infrastructure-as-a-Service provides "servers, operating systems, applications, databases" and allows the user to control "all aspects of the infrastructure" (Ibid). IaaS providers include Amazon Web Services and Infocrossing.

The most successful of all Cloud Computing projects thus far, and the one to which almost all other cloud computing initiatives are measured against has been Amazon's EC2, also known as the Elastic Compute Cloud. EC2 allows you to rent a virtual computer by the hour, as many as you need and as often as you need then, hence the term 'elastic'. EC2 grew out of Amazon's experience and investment in large-scale IT infrastructure (Amazon Web Services 3). Today, EC2 enables users to 'spin-up' a virtual instance of Linux, Windows Server, and several other operating systems, and utilize your own software or predefined packages including

databases, web servers and disk storage. EC2, along with other cloud offerings from other vendors, isn't trouble-free. It relies on the Internet for access, which can be subject to an errant backhoe digging up a fiber optic communication circuit, a poorly-planned router software upgrade or even sun spot activity for wireless users. Amazon's EC2 was down for many customers in April, 2011 for several days, prompting Matthew Eastwood, a research firm analyst to say "This is a wake-up call for cloud computing" (Lohr). Just after midnight on April 21st, Amazon's EC2 status dashboard began reporting various failures affecting its storage system, the relational database system and several applications. Arik Hesseldahl's article on the All Things Digital website entitled 'Amazon's Cloud Crashed Overnight, And Brought Several Other Companies Down Too' (Hesseldahl) detailed a running diary of Amazon's status messages to its customers, which include popular social networking site FourSquare, The Cydia Store, an alternative app store for the iPhone and other Apple devices, and many others. One analyst stated "When this kind of thing happens, it definitely sends a chill through the whole cloud and hosted services industry" (Gaudin).

The Amazon incident came just days after Sony experienced 'a nightmare of a security breach' (Konstantas). Sony shut down its entire online gaming network after discovering hackers had infiltrated its computer network, comprising personal and financial data of up to 77 million of its customers. Sony downplayed the breach at the time as relatively minor, indicating that only an outdated database was hacked into. Still, Kazuo Hirai, a Sony executive deputy president in charge of consumer products and network services stated "We have to regain the trust and confidence of our users" (Edwards and Riley). The PlayStation Network was subsequently unavailable to its users for more than three weeks, not returning online until May 14th. In its aftermath, it is unknown exactly how many customers were at risk for identity theft, email

spamming or other potential abuse of their supposedly confidential and secure personal information.

Another very real danger is the server your application and data resides on being repossessed by a creditor, or being confiscated by law enforcement. In June 2011, the FBI raided a data center in Dallas, seizing computers of not only the suspect's, but of several innocent tenants sharing the same rackspace (Blankenhorn). With the increased use of blade computers, which may share a host chassis, as well as virtualization, this could be a growing concern for cloud customers. If you're running an application in the cloud and another company sharing the same server gets into legal trouble, "the entire physical server could be subpoenaed, which would mean that you wouldn't even know what happened," says Matthew Sarrel, an IT consultant and contributor to PC Magazine. "It would just be gone" (Neuman). Also of concern is the locality where your data is being hosted. When contracting for cloud services, it's important to know where the data center is located where your applications and data will be hosted from. For example, if your company is a defense contractor, you may need to ensure your contract specifies that your services are provided wholly within the United States, and that only U.S. citizens have access to the servers which are hosting your data, lest the government of an unfriendly nation 'nationalize' your data. And US laws give similar pause to companies based in other countries. Purdue University computer science professor Eugene Spafford says that "Many companies in Europe are concerned about their data being on cloud servers in the United States because the Patriot Act allows the government to snoop on records."

Even still, cloud computing continues to grow more popular. Customers have options available to reduce the risk of placing all of their eggs in one virtual basket. Many providers, including Amazon, have redundancy options, which allow the customer to decide which

datacenters, and how many their services are provided from. Most importantly is that customers be aware of exactly what services are being provided to them, and where, and that they continue to safeguard their own data, by using multiple providers at minimum, and preferably by maintaining their own backup copies of all of their data. Cloud technology is an often misunderstood or even foreign concept to many people, even those who regularly use computers. It's important to keep in mind that with all the efficiencies achieved by using cloud services, the same concerns regarding data security, accessibility and availability remain.

Works Cited

Amazon Web Services. "Overview of Amazon Web Services." n.d.

Blankenhorn, David. "Commentary: Not knowing where your cloud is could lead to stormy weather." 7 August 2011. The Washington Post. 28 November 2011 <http://www.washingtonpost.com/business/capitalbusiness/commentary-know-who-controls-your-cloud-data/2011/08/03/gIQAU26w0I_story.html>.

Bragonier, Dwayne. "Still Foggy on Cloud Computing?" CA Magazine September 2011: 26-35.

Dimitrios Zissis, Dimitrios lekkas. "Securing e-Government and e-Voting with an open cloud computing architecture." Government Information Quarterly (2011): 239-251.

Edwards, Cliff and Michael Riley. "Sony Data Breach Exposes Users to Years of Identity-Theft Risk." 3 May 2011. Bloomberg Businessweek. 28 November 2011 <http://www.businessweek.com/news/2011-05-03/sony-data-breach-exposes-users-to-years-of-identity-theft-risk.html>.

Gaudin, Sharon. "Amazon gets 'black eye' from cloud outage." 21 April 2011. Computerworld. 28 November 2011 <http://www.computerworld.com/s/article/print/9216064/Amazon_gets_black_eye_from_cloud_outage?taxonomyName=Cloud+Computing&taxonomyId=158>.

Hesseldahl, Arik. "Amazon's Cloud Crashed Overnight, And Brought Several Other Companies Down Too." 21 April 2011. All Things Digital. 28 November 2011 <http://allthingsd.com/20110421/amazons-cloud-crashed-overnight-and-brought-several-other-companies-down-too/>.

Konstantas, Johnnie. "What Does the Sony PlayStation network Breach Teach Us about Cloud Security?" 30 June 2011. SecurityWeek. 28 November 2011 <http://www.securityweek.com/what-does-sony-playstation-network-breach-teach-us-about-cloud-security>.

Lohr, Steve. "Amazon's Trouble Raises Cloud Computing Doubts." The New York Times 23 April 2011.

Neuman, Scott. "Experts Warn Of Turbulent Trip To Cloud Computing." 14 June 2011. NPR. 28 November 2011 <http://www.npr.org/2011/06/14/137174402/experts-warn-of-turbulent-trip-to-cloud-computing>.