

Plenty of Amazon Outage Blame to Go Around

By: Mike Vizard

April 26, 2011

CTO Edge

There's been a lot of pointed criticism leveled at Amazon specifically and cloud computing in general as of late following recent high-profile outages that have affected some fairly well-known sites. Much of the criticism is well-deserved. But what seems to be escaping everyone's mind is some of the questionable decisions that the IT organizations made when ultimately deciding to rely on the Amazon public cloud computing service.

The first issue that comes to mind is how overly dependent these organizations are on Amazon. There is nothing in the annals of computing that would suggest that just because an IT service is in the cloud that it is not subject to the same issues that affect IT infrastructure running on premise. While it's true that one might expect that Amazon would have done a better job of getting customer sites back up and running, the fact of the matter is that IT INFRASTRUCTURE is subject to failure. What is just as surprising as Amazon's inability to quickly resolve the problem is the IT organizations that relied on Amazon didn't appear to have much of a contingency plan in place to deal with such an ordeal.

Abhik Mitra, a product manager for Kroll Ontrack, a provider of data recovery and backup tools, says one of the big issues with any public cloud computing service these days is the assumption that somehow the availability of the public cloud computing service is guaranteed. However, when you look closely at the service-level agreements (SLAs) provided by these providers, they typically say things like 99 percent availability. Well, that 99 percent availability, depending on the size of the overall site, might equal two weeks of actual downtime a year. And as a fellow named Murphy likes to constantly remind us, the odds are that at least one of those days is going to affect your business. The other issue that too many IT organizations ignore, adds Mitra, is making sure recovery that goes beyond a "best effort" clause is spelled out in detail.

Ultimately, it's your organization's data that is stored on the public cloud service. That means the internal IT organization is still responsible for managing it, including putting in place all the backup and recovery processes required. In an ideal scenario, there would be virtual servers either on premise or in another cloud that would be ready to take over for the affected servers on a moment's notice. Of course, that would mean that IT organizations have a proactive approach to data management in the cloud in place.

There's no doubt that Amazon's woes over the past few days are a black eye for public cloud computing. But in general, most internal IT organizations have more outages than an external provider. Those outages just don't get as much publicity because they don't affect multiple customers at the same time. But when those outages do occur, there should be plenty of blame to go around both inside and outside the IT organization that ultimately selected a public cloud computing service without putting the proper controls in place to deal with availability issues that are bound to occur.