DR Blog Series, May 2013
EvolveIP, FINAL [1,194 Words]
How Moving to the Cloud Can Help Businesses Avoid Disaster

Disaster Wake-up Call: Can Moving DR to the Cloud Really Safeguard Your Business?
By Guy Fardone

Read this statistic carefully: 93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy; 43% never reopen…according to FEMA's latest findings (March 2013).

Now read it again, but recall the countless record-breaking cataclysms of the last 24 months.

From furious hurricanes to terrorist bombings, from global flooding to epic droughts in the Midwestern US, and from bone-rattling earthquakes around the world to month-long wildfires…disasters seem to be just a hair's breath away these days.

But, you think confidently, you have a Disaster Recovery (DR) plan in place. You may already back up your data on tape or even better yet, off site. Maybe you have some services in "the cloud" so you won't be another sad statistic. You're in pretty good shape.

That's what many companies in the northeast US thought too, but seven months ago Hurricane Sandy smacked them with a reality check that has left many still stinging with open wounds.

The freak storm forced 74% of small business owners in New York City, New Jersey, and Connecticut to close their doors. Another 71% of small to medium-sized businesses owners lost power as a result of the storm, while most lost phone, WAN and internet connectivity. "Loss of connectivity had a big impact on small to medium-sized business owners," said Ray Sprague, senior vice president of the Small Commercial insurance segment for The Hartford, which conducted the research. "We have found that small businesses that take the steps to prepare and protect themselves, such as establishing emergency communication systems and backing up critical data, are the ones that prevail after emergencies."

It's time to get smarter. First off, let's stop thinking in terms of 'recovery' and more in terms of 'avoidance' so that companies – large and small – can save their skin. How do you get there? One of the most efficient ways is by leveraging the cloud with best-in-class, cloud-based technologies that protect your data and communications assets so you can truly avoid disaster…not just recover from it.

Here are three ways moving to the cloud with the right cloud provider helps:

● Environmental Protection: If a company's on-site data center loses power or employees cannot access the physical building for any reason, the business may stop or significantly slow down. Applications that are run in the cloud and off-site, and properly backed-up in various locations, on the other hand…enable an "always-on" environment. In other words, your business applications are always

accessible from anywhere, any time so if your company's power goes out or your employees can't get there because of road conditions, then they can simply work from home or other safe location.

● Network Protection – If power is out, network is generally out. But networks can still be down when power is restored. (Just ask any Verizon customer located in Hurricane Sandy's path about service interruption...even today, seven months after it hit!) Aging infrastructure or poorly architected network hubs can wreak havoc on your networks, and consequently, your customer service levels. In contrast, networks in the cloud – if architected properly – provide companies with various pathways to access their network data and applications.

● Business Applications & Data Protection – Your business operating plan for all of your applications and systems including your CRM, databases, email, computing infrastructure, phone systems, call centers, and others should follow three key guidelines that translate into Service Level Agreements to internal and external customers. These are Recovery Time Objective (RTO) or the maximum duration of time allowable for complete restoral after a disruption to an acceptable level of business continuity; Recovery Point Objective (RPO) or the maximum tolerable period in which data can be lost (from its last update); and Network Uptime Objective or the percentage of time a system, network or application should be available or 'up.' In each case, industry standards provide a benchmark for what's acceptable.

For example, the minimum goal for Network Uptime should be 99.9% on core applications which translates to less than 45 minutes of downtime per month. Lifesaving businesses such as hospitals and those that are heavily dependent on their systems may need to target 99.99% or perhaps even "5 nines," which is 99.999% uptime or less than 5 minutes of downtime per year.

Meeting basic Uptime, RTO, RPO objectives is difficult enough, while meeting even more stringent objectives is practically impossible using traditional on-premise systems. However, leveraging a cloud architecture in whole or in part substantially increases the ease, efficiency and probability of meeting these objectives regardless of the type of business or how critical the applications.

But, Is the Cloud Enough?

In Marvel's newly released "Iron Man 3," Robert Downey Jr.'s snide Tony Stark builds a whole new fantastical suit of iron – wildly fitted with high-tech gadgetry that empowers the hero to fight evil. Tony thought of everything when he designed and built the suit with an "N+1" architecture in mind so that nothing would go wrong. Likewise, for the cloud to really do the job of protecting your data, applications and communications systems from peril, the provider must be similarly suited. In other words, the cloud needs more than just the cloud to fully support your Disaster Avoidance strategies.

Here are a few quick tips to help evaluate potential cloud providers:

- The right cloud provider must have invested in geographically disparate data centers. Period. There is no other option.
- These data centers much be physically safe (think no flood or earthquake zone and secure access).

- The right cloud provider must have world-class technology centers for its infrastructure – complete with dual power grids, multiple battery lines, emergency generators, back-up fuel supply, an advanced fire-suppression system, VESDA smoke detection and thermal detectors, a fail-safe alarm system, adequate cooling and ventilation, and more.
- The right cloud provider must have 'active active' connections with network providers so that if one provider is down, another is up. If any one of the upstream providers goes down, the others stay running and so does your company. In fact, the more connections, the better.
- Of course, the provider should also demonstrate that it regularly does preventative maintenance on all of its systems.

Finally, the 'Iron Man of cloud providers' must employ certified experts and processes that have been drilled repeatedly with tangible, proven test and control processes. Mission critical and compliance regulated organizations will need an even greater sense of security and will need to look for third-party audited service providers with compliance focused around SSAE, SOC, PCI or HIPAA.

Despite the growing number of bandwagon cloud providers that are trying to leverage the cloud trend, success still comes down to smart people who are skilled and prepared. Technology is a great enabler but it's the people and processes behind the curtain that make the difference. At Evolve IP, we work with you and your DR team to help develop a failsafe plan that avoids disaster, whether that's just a brief power outage or widespread disaster. Download a thorough DR checklist here, and then talk to us about cloudsourcing your critical systems to Evolve IP to eliminate concern that a disaster will affect your business.

Its Disaster Avoidance fit for super heroes.

###

Sources:

1. National Archives & Records Administration in Washington DC

2. Business Week, http://www.businessnewsdaily.com/4168-superstorm-sandy-small-business-impact.html