



The Role of The Cloud in Disaster Recovery Planning

Disaster Recovery, Business Continuity, and
Storage in Cloud Computing Environments

June 2010
Kristoffer Sheather
Cloud Central
www.cloudcentral.com.au

Introduction

Nobody likes to spend money for something that may never get used, but that's the very nature of disaster recovery and business continuity strategies. You spend money on a system you hope you will never use, but if you do use it, it could save you millions.

After a major disaster, it is common for companies, especially smaller companies, to close their doors forever. Not because they were poor companies, or unprofitable, or didn't have customers—only because they couldn't get up and running again quickly enough after the disaster, and they lost their forward momentum.

Traditional disaster recovery involves fully redundant hardware, regular backup of data, and in the case of some important information such as transactional data, a two-phase commit. It's expensive, it takes a lot of planning, and it doesn't even always work the way it should. A cloud-based disaster recovery strategy has become a viable and less costly alternative. Companies that operate their data centres in the cloud already have an advantage in the event of local disaster, since their servers, data and applications are no longer localized; companies that use the cloud as their redundant infrastructures avoid the otherwise high costs of redundant hardware and dedicated off-site facilities.

Definitions

Disaster recovery, business continuity, and storage/backup represent three different but intersecting areas of technology. The biggest mistake is to believe that since you back up your files on a regular basis, then you are prepared for disaster recovery and business continuity. In reality, that's only the beginning. Let's take a look at what these things mean.

Data backup is the foundation of good business practice, but there are many ways to create extra copies of your files. A smaller business may simply back up files to a CD or external hard disk, or a larger one may back them up to a redundant storage server. A better strategy though, will take into account what would happen in case of disaster. When your primary facility is struck by flood, fire, or earthquake, if you've kept those backups in the same office as your main computing environment, then they are of no use. Keeping those backups in an external facility, or sending them to a third party cloud provider, starts to take disaster recovery into account.

Disaster recovery is a strategy, backed by technology, that allows you to get up and running quickly after a disaster. Business continuity, on the other hand, is the strategy that allows you to continue operating under emergency circumstances after the recovery has taken place.

For example, when your headquarters and data centre have suffered a disaster, but your data and applications continue to be available through your cloud provider, you have a sound disaster recovery plan. But figuring out what to do with it and how to deliver access to all of your staff is business continuity.

Strategy and Technology

Getting ready for disaster starts long before you even consider technology. It is first a strategic consideration, and the biggest step to being prepared is to create a written disaster recovery plan.

Cloud Central - The Role of The Cloud in Disaster Recovery Planning

This is all about knowledge—knowledge of what you have, and what you will do if it's lost. And what do you have? You have people, an office, and computers, usually all in the same physical location. Let's take a look at what to do with all three of those assets if your physical location is no longer available.

People. Having a redundant system won't do any good if your people can't access it. Good planning calls for a strategy to make sure that your staff has the information they need to access your system after a disaster. The written disaster plan creates a strategy for knowing where your people are, and how to reach them. A master personnel list, with names, street addresses, phone numbers and email addresses, needs to be accessible and off-site, perhaps in a safety deposit box, so that your appointed "disaster officer" can relay information to staff on where to go and how to proceed.

Office. You have contacted your staff, but now where will they go? Work still needs to get done, but the office is unavailable. The second part of the disaster preparedness triad addresses just where the work will get done. It may be as simple as getting everybody together in the CEO's home, or having a contingency agreement with a facilities company for alternative space. A cloud-based disaster recovery plan allows for a more workable option, which is to allow all staff members to work from home, or whatever nearby facility may be available.

Computers. Almost any company today depends on its computers for survival, and the plan needs to include a strategy for continuing to have access to the data and applications that were housed on the computers in your office. You may have successfully contacted your people and figured out where they can work, but without computers (and the applications and data that resides on them), you're at a standstill. The traditional approach would have been full redundancy and off-site data centre's, often too costly for smaller businesses. A cloud-based solution provides a solution, by establishing full redundancy through the cloud, without having to bear the expense of purchasing redundant equipment.

The virtual office and remote working

Fire, floods, earthquakes, killer bees—you name it. The possibilities are endless. Something, or somebody, could disrupt your operations and render your headquarters unusable. Your disaster recovery plan must include a strategy for alternative workspace. In the past, forward-thinking companies may have addressed this need by contracting with a facilities management company to provide office space at a moment's notice in case of disaster. Using this strategy, the alternative physical space would be immediately available, and possibly even already equipped with computers and office furniture.

There are two downsides to the alternative physical office space strategy: First, it is potentially very costly, and second, if the alternative physical space is in the same town as your now-inaccessible office, there is a chance that the alternative physical space would have been hit by the same disaster. Roads may be inaccessible, and some staff members may have had to abandon their homes and seek temporary lodging in other towns. Getting everybody together after a disaster is logistically difficult and often impossible.

Cloud Central - The Role of The Cloud in Disaster Recovery Planning

The “virtual office” concept provides a workable alternative. A written strategy, some education that instructs all personnel on access methods, and a good cloud provider means you can “take the company virtual” within minutes, and be up and running at full speed while your competitors are still trying to figure out what to do.

Cloud computing, and the “virtual office” concept that it has enabled, has an answer to all three strategic concerns (people, office, computers). Your people can be reassured that they can continue working after disaster occurs. The office? The physical limitations of cubicles and office buildings are fast becoming obsolete. Basic conferencing and collaboration equipment makes it possible to work efficiently and collaborate without ever being in the same physical location. But of course, we still need computers, but the servers, storage arrays, data and applications that run the company don’t have to be in the same physical space as the people who run them.

A virtual office is used by many small companies with geographically diverse staff under normal circumstances; under disaster circumstances, the virtual office fills the need to keep business going. On the policy end, all employees need to either have computers in their home, or access to one; and knowledge about remote login procedure to the corporate cloud. The damage done by a localized disaster is kept to a minimum, because the company is no longer dependent on what is available locally. The office may be completely inaccessible, but as long as there is Internet access available, staff members can log onto corporate applications from anywhere, from any computer.

Disaster recovery and SMEs

While most larger enterprise companies will have at least paid tribute to the concept of disaster recovery and business continuity, small and midsize businesses less likely to have such a plan in place. It’s not because they are any less savvy, the main factors are time and money. Traditional disaster recovery can be costly, and a smaller business may not be in a position to write those big checks.

The cloud has become attractive to small and midsize enterprises for several reasons. A survey conducted by the European Network and Information Security Agency (ENISA)¹ asked what the reasons were for a possible cloud computing engagement. Not surprisingly, the most popular response was to “avoid capital expenditure,” with 68 percent of respondents indicating their main motivation for cloud computing was one of dollars and cents. But the third highest response at 53 percent was to gain access to business continuity and disaster recovery capabilities.

With a majority of SMEs looking to the cloud for business continuity and disaster recovery, it’s easy to draw conclusions: Smaller businesses have historically lagged behind in implementing these strategies. But although they have lagged behind, it’s not out of ignorance. Most small business owners and executives realize the need for disaster recovery, but have seen it as too costly—until now. The cloud will bring more SMEs into the disaster recovery fold, giving them a greater opportunity to be prepared, and a greater chance of surviving a disaster.

Deployment of disaster recovery

¹ European Network and Information Security Agency. “An SME perspective on cloud computing survey.” November, 2009.

Cloud Central - The Role of The Cloud in Disaster Recovery Planning

Disaster recovery scared away many smaller businesses because of the time and cost factor, and the impression that disaster recovery was only something that huge companies needed to do. Fortunately today, that is no longer the case. Instead of taking several weeks to deploy, a new server (redundant or otherwise) can be deployed in several minutes, and without the up-front capital cost of equipment.

Using cloud computing as the foundation of disaster recovery is a simple process. A virtual server in the cloud can be provisioned in just a few minutes, and easily configured to mirror your own internal production environments. Synchronize your internal data with your cloud environment on a regular basis, and you have a fully redundant infrastructure without having to pay for extra hardware and a dedicated off-site facility. The cost of disaster recovery preparedness suddenly becomes affordable to even the smallest business. Larger businesses too will benefit from this approach, which helps them to avoid diverting valuable IT resources to managing redundant systems and instead focus on more pressing tasks.

Post-deployment, regular testing of your redundant environment is essential. Backup may be unreliable or may fail on occasion, and so regular testing to ensure that your mirrored applications work as they should, and that your data is recoverable and fully accessible. If you use the cloud in your day-to-day business, then your staff members will already know how to access their data and applications from any computer. But if you are using the cloud for backup and disaster preparedness only, staff members may be unfamiliar with the process, and so education here is critical.

You're prepared for disaster, but is your cloud provider?

Once you have taken the appropriate steps to implement your disaster recovery and business continuity strategies, you will have already made a few decisions regarding cloud computing. Cloud computing can play a major role in these strategies, but the big question is, what happens when your cloud provider suffers a disaster?

Your cloud provider is now holding redundant copies of your data and applications, providing you with a viable way to get up and running after the worst happens. But what if the worst happens to the cloud provider too, what happens to your data?

The answer is simple, and that is the cloud provider will have disaster recovery strategies of their own. Or at least, they should, and this will be a major factor in your selection process.

In most cases, a reliable cloud provider will already have redundancy and backup built into their own systems. While this is certainly an area to ask about before buying the service, it has come to be expected. Your cloud provider will offer you a service level agreement; pay careful attention to the details of this document. This will not only specify service expectations in terms of uptime, accessibility and reliability; it will also lay out details on what you can expect in terms of recoverability should your provider go out of business or suffer a disaster of their own.

In your selection process, understand that the term "cloud" doesn't necessarily mean that the actual location of the provider's servers is unknown. Where are your provider's physical assets? Knowing where that data centre is located is an important part of the decision-making process. Your provider may have assets in their own data centers or collocation facilities, and may well have multiple physical locations. While using a cloud provider that is your next-door neighbor is a poor idea for obvious reasons—the disaster that affects you will affect them as well—having a cloud provider that

Cloud Central - The Role of The Cloud in Disaster Recovery Planning

is too far away will also bring problems of latency, cross-border issues of compliance with local statute, and lack of accountability. A cloud provider in your home country will be the most advantageous to your DR strategy.

Conclusion

Disaster recovery is no longer a luxury restricted to large companies with deep pockets. Smaller businesses can be protected too by incorporating cloud computing into their disaster recovery and business continuity strategies. A complete disaster recovery plan takes into account people, offices and computers, making a strategic plan to accommodate all three. A cloud-based disaster recovery strategy overcomes the limitations a company may face in trying to obtain centralized office space after a disaster, while also providing continued access to data and applications. And most important, it can be done quickly and affordably.