5 Steps to Prepare a Disaster Recovery Plan

HopOne Internet Corporation

An information technology (IT) disaster recovery (DR) plan provides a structured approach for responding to unplanned incidents that threaten an IT infrastructure, which includes hardware, software, networks, processes, and people. Protecting your firm’s investment in its technology infrastructure, and protecting your capacity to conduct business are the key reasons for implementing a DR Plan.
Chapter 1

Introduction

Information Technology easily can read like a Tom Clancy novel – until you realize that this is not some kind of made-for-TV movie or summer best seller. It is real and it could strike close to home – it could happen to your company.

In June 2011, potential disaster struck the U.S. Department of Energy facility in Las Alamos, New Mexico. A fast moving wildfire had moved within a mile of the southern part of the lab facilities and all non-essential personnel were evacuated. This facility houses two of the most powerful supercomputers in the world, the Roadrunner and the Cielo computers.

Fortunately a combination of firefighters and rain helped push the fire away and it was eventually put out, however, what would have happened if the fire continued in that direction and disaster had struck?

Now, no doubt your company or organization does not house a nuclear plant or supercomputers, however, it is still important for you to have disaster recovery management systems in place that will allow you get back up and running in the event of a disaster.

When companies are hit by disasters, certainly their physical facilities can be damaged and sustain huge physical losses – however, most companies realize that the even larger cost is in potential data losses that, if recovered at all, could take months, thereby putting the entire business organization at risk. Such data losses can even, in some cases, lead to additional law suits and litigation fees. Although it is important to implement a DR Management Plan for your physical facilities this report will center on the IT or data piece of implementing a DR Plan.
Chapter 2

What is a Disaster Recovery Plan?

What exactly is a disaster recovery plan? It is a plan that provides step-by-step procedures for the recovery of data, systems, and networks, then helping them to return to normal operations.

Whether you realize it or not, all companies – actually all computers – need to have some kind of disaster recovery program in place. It could be as simple as backing up your computer’s files weekly to developing and implementing a fully documented DR management plan – it all depends on the size and needs of your company or organization…as well as the ability to easily recreate any data that has been destroyed when the disaster strikes.

The question in many people’s minds is why their company should even have a DR plan in place? After all, it is quite easy to tell everyone to back up their computer once a week and make each employee responsible for their own data. So I guess it boils down to this: are you willing to trust your employees with your business? If so, then you’re quite the gambler!

A study done by the University of Texas found that 43 percent of companies that experience a catastrophic data loss will never re-open its doors. Another 51 percent will close within two years of that catastrophic event. Only six percent of companies that experience a catastrophic data loss will recover and survive. So if you are not willing to put a data recovery management plan in place, then you are taking a huge risk.

If you are reading this and these percentages do not alarm you, then you probably either have a very strong constitution or, hopefully, you already have implemented an effective data recovery plan there.
Chapter 3

The Five Steps of a DR Plan

What happens if your company or organization does not have a DR management plan in place or the plans are not in alignment with company requirements? If this is the case, then here are the five things that will put you on the right path in implementing a DR Plan.

• Create a Disaster Recovery Management contingency statement for your company or organization.
• Conduct a Business Impact Analysis (BIA)
• Identify measures and controls
• Create recovery strategies including an IT contingency plan
• Implement testing, training, measuring, and maintaining the plan
Chapter 4

Disaster Recovery Management Contingency Statement

So what exactly is a DR Management Contingency Statement? It is a formalized policy or set of guidelines that authorizes a DR plan to be developed and implemented. Is this a policy that should be set in stone? Absolutely not. A DR recovery plan should be a “living” document. IT, data, networks within companies are constantly changing and evolving. Even a software update changes the dynamics of your IT systems, therefore, the structure of the plan needs to have flexibility built into the system.

When developing a DR Plan, it is important to understand the implications of each department involved and how they mesh together. Therefore, it is critical that a team is created and not just one or two people to get involved. This team is accountable for:

1. Determining the scope of the plan (including both internal and external elements and assets), choosing third-party vendors and systems, and briefing senior management.
2. Assembling all the documentation necessary to develop a relevant DR Plan. This includes compiling network diagrams, systems documentation, and configurations for equipment.

Identifying the following and then compile and document the same:

- What are the serious threats to infrastructure – both natural and man-made? This could be power system failures, human error, fire, etc.
- What are the most serious vulnerabilities?
- What is the history of any previous disruptions?
- Prioritize the most critical areas that must be back up and running first.
Chapter 5

Conduct a Business Impact Analysis (BIA)

Throughout the process of developing a Disaster Recovery Management Plan, it is common for many of the processes to overlap and morph together – and it is natural. One of the reasons for this to be a flexible plan is because there are constant changes within most companies or SMB organizations. But creating a DR Plan should never be a case of the blob that ate your company. So, when you are creating the plan, keep in mind the scope of the work and create a timeline with several built-in phases. This will allow your team to track their own progress and will help senior management to keep informed.

After the DR team has gathered the relevant information, it is time to create a business impact analysis. This BIA is used to determine how the risks that were identified will have effect your business operations. When an incident negatively impacts business ops, your company will be affected and the consequences could be disastrous.

A business impact analysis helps companies and organizations to identify their priorities and create, modify, and validate plans for the company.
Chapter 6

Identify Control Measures

Within the disaster recovery plan, one of the most important areas is identifying control measures and eliminating threats. What are control measures? They are the steps that are implemented to reduce threats to companies.

For example, often employees are allowed to visit almost any Internet site from their company computers. When there are no structures placed on their surfing, this can open the company servers up to the possibilities of viruses, malware, and other disastrous possibilities. By filtering the websites that employees are allowed to visit, a company can reduce the possibilities of viruses or malware potentially contaminating their systems.

This is just a small example of how a control measure can be implemented to keep your company’s data safer and more secure and to reduce the potential of a disaster striking. The three types of control measures that can be implemented:

1. **Detective measures**: Controls that will detect and discover events.
2. **Preventative measures**: Helps prevent an incident from occurring.
3. **Corrective measures**: Rectifies or restores a network or system after an incident occurs.

When your company or organization has identified and implemented control measures, they should be documented, updated, and tested on a regular schedule.
Chapter 7

Create recovery strategies including an IT contingency plan

So what happens if a disaster strikes your company or organization? No one wants this to happen however, if the worst comes to worst, you can soften the impact with recovery plans. Each department in your company or organization should have a set recovery strategy as well as a well-defined and understood priority list set in place. **Identify the critical departments and areas of each department that are crucial to a company’s ability to get back up and running with minimal impact on the business.**

Some of the most common strategies for a company should be data protection. Backups should be made frequently (often daily) and the data should be sent off-site. The most common backup are to tape and disk (on-site as well as off-site). It is also crucial for the back-up information to be tested regularly so that data won’t be lost in the event that it is needed. There are some excellent high availability systems on the marketplace that keep data safe.

Many companies or organizations choose to outsource their data recovery to an outside provider since the providers are dedicated to data management and are very affordable.
Chapter 8
Implement testing, training, measuring, and maintaining the plan

As mentioned previously, it is critically important that after you have developed and implemented DR Management Plans...that they are maintained. Just as you would not spend the time, money, and energy to visit the doctor for an illness, then just disregard his advice and let the medicine he prescribed sit on your bathroom shelf...okay, maybe some of you would but you understand what I am getting at here...it is important to treat your DR Plan as a flexible, ongoing plan.

Set a timeframe for the disaster recovery management team to meet – perhaps on a bi-annual basis – to review the priorities of each department. It is also important for not only the team and senior management to be aware of the plan, but also each employee to be trained about their part of the DR process.

Involving all your employees in the DR management process will ensure that they are aware of what is necessary to keep their company or organization running smoothly but also help it recover quickly in the event of an emergency.
Chapter 9

Wrap Up

No one wants a disaster to happen, however, creating an effective disaster recovery management plan for your company will go a long way in helping you stay in business in the event of a disaster.

For a free Disaster Recovery Plan Template just ask me! Otherwise was can also help with DR Plans and especially in housing your DR site infrastructure within our certified and audited data centers coast-to-coast.

Have comments, questions, or feedback? Just let us know! Northern Virginia:

DCA2
8201 Greensboro Drive, McLean, VA 22102
Tim Sexton
tsexton@hopone.net
571-282-6321 office / 571-426-9824 mobile

DCA3
6621 Electronic Drive, Springfield, VA 22150

CLOUD COMPUTING GIVES COMPANIES THE OPPORTUNITY TO RETHINK MANY TRADITIONAL IT PRACTICES, BUT IT IS PROVING A PARTICULARLY GOOD FIT FOR DISASTER RECOVERY & BUSINESS CONTINUITY … SEE FAQ ON SAME NEXT PAGES:
Disaster Recovery Services

Every business should have a business continuity plan in place. Not an idea, but a well-evaluated and detailed course of action to ensure that their business can get through a disaster and continue on in the aftermath. This plan included crisis management, business procedures/processes, and work area management to name a few considerations.

Another important, yet often overlooked part of your business continuity plan is IT disaster recovery (DR). In broad terms, this is how you deal with and prevent IT downtime. Even if every other part of your business continuity plan is executed perfectly, you remain at a standstill if your IT systems go down and stay down. And the situation will only get worse as your revenue and reputation take a beating.

Remember, disaster recovery is not the same as disaster prevention. There’s a huge difference between disaster prevention and disaster recovery. Both are necessary. But the former only mitigates the risk of downtime. The latter makes sure if downtime happens, you can actually get your IT back online quickly.

Wondering how much an outage could cost your business? These calculations can help:

**ANNUAL REVENUE**

Take the annual revenue number and determine what percentage of that revenue comes from online. That total annual online revenue number can be multiplied by the number of high-revenue hours per day your business experiences, which would allow you to estimate an annual number of total revenue hours. From there you could determine the cost of downtime per hour to your business.

**EMPLOYEE PRODUCTIVITY**

Take that annual revenue number and divide it by the number of employees within your business. That gives you the average revenue per employee number. Take the total work hours per year in hours, the employee revenue per hour in dollars, and the actual number of hours of downtime to figure out the percentage of employees affected by downtime. From there you can determine the cost of downtime per hour to your business.

Many companies learn the hard way, how important DR is to IT and their business overall. Betting on never experiencing a service outage or a natural disaster is not a viable or practical choice. The stats tell the story.

- 43 percent of companies experiencing disasters never reopen, and 29 percent close within two years...according to McGladrey and Pullen
- 93 percent of businesses that lost their datacenter for 10 days went bankrupt within one year...according to National Archives & Records Administration
- 40 percent of all companies that experience a major disaster will go out of business if they cannot gain access to their data within 24 hours...according to Gartner
Disaster Recovery FAQs

What are the different roles the cloud can play in disaster recovery and business continuity?

Probably the most basic thing is backing up data offsite. Most large companies have some sort of a backup strategy, but more often than you might think we find companies who are not sending their data offsite or not sending it far enough offsite. When we ask if they have checked to see what potential regional issues they might have, sometimes they find some geological or weather or some other type of potential risk that would affect their ability to recover locally; the cloud gives them the ability to store data some place remote, store it online, and to typically recover faster than from tape.

Then there are services that allow clients to fail-over servers. The cloud is very good now for Wintel servers, where you can replicate your data and fail-over relatively quickly. So in addition doing replication of data to another server, we still recommend backup because you can recover individual files to a point in time. With server replication you will fail over, but you may not be able to go back as far as you want unless you’ve got a facility such as our Virtualized Server Recovery, which allows you to take snap shots.

So the cloud gives companies backup of data, fail-over of servers, and the ability to have a secondary center far enough away to allow for regional disaster recovery. And one other thing I should mention, the cloud also gives companies the ability to store their business continuity plans offsite. I know it seems like a nit, but you’d be surprised how often business continuity plans are lost in a disaster. Those plans are critical and if they’re stored on a system in the primary center, how are you going to run the recovery if you can’t get to that system? The cloud gives them the ability to store those plans and the notification scripts on a server they can access from their laptop anywhere they can access the cloud, like a Starbucks. And for a business continuity manager that’s critical to their success.

**BENEFITS:** CLOUD COMPUTING DELIVERS FASTER RECOVERY TIMES AND MULTI-SITE AVAILABILITY AT A FRACTION OF THE COST OF CONVENTIONAL DISASTER RECOVERY.
Larger companies take business continuity seriously and have comprehensive plans in place, but for companies that could do more does cloud offer enough advantages to get them off the dime?

The cloud gives small and medium-sized business the same capabilities that larger companies have had for years. Many larger companies have secondary data centers they can use for data backup and recovery, whereas most small companies don’t. Smaller companies – with, say, 25 to 100 servers – very often back up to tape and maybe they store the tapes locally and they may not have a sophisticated disaster recovery plan and strategy. Now, the cloud gives them same capabilities as large companies. They can back up data or replicate servers to a remote site, and then fail-over the servers and network to the remote site in the event of a disaster. So it’s giving small and medium-sized businesses much more sophistication.

How about for the higher-end folks that do have sophisticated plans in place, are they looking to the cloud as well?

For companies that have sophisticated disaster recovery architectures and strategies, introducing the cloud can be beneficial from a financial perspective and from a control perspective, because with cloud disaster recovery you get to test it more often. But larger companies are asking, “How do I integrate this into what I already have? I test twice a year. I take those tests and I give them to my auditors. How am I going to do this now with the cloud? And by the way, I might have some technology that can’t be recovered into the cloud. So how do I do that?”

The larger companies need to create an integrated strategy of processes, architecture, and the reporting necessary to demonstrate to auditors they have this capability. One of the benefits of having a consulting group like ours, is that we, unlike some other cloud providers where you’re on your own, can consult and create that strategy to enable cloud to work with what you have.
When you're talking to larger companies, where do you get started?

It depends upon what they have. Some organizations are do-it-yourselfers. They have a sophisticated plan and they know how to implement it. They may say, “All we want from you, HopOne, is your Cloud Managed Backup, or your Cloud Virtualized Server Recovery or your Cloud Content Manager. Just give us the cloud services and we’ll do it. Then we have other customers that want some help setting it up. First thing we say is, show us what plans you already have and we can work together to create the strategy, architecture, processes and procedures necessary to ensure success with integrating cloud into the disaster recovery capabilities of your company.

What are the expectations of cloud? Is it easier to set up, faster to implement, less expensive?

There are some cost implications because remember, we’re using a cloud in a shared environment, as opposed to a customer having a dedicated technology sitting on their floor. So for some it’s a matter of OPEX vs. CAPEX, with OPEX may be a little more attractive to the customer. But, frankly cost is only a small part of it. Companies are looking at flexibility. The flexibility to test more frequently and the ability to scale up or to scale down if needed. Those are the kinds of reasons clients are trying to introduce cloud into their environment.

Average Downtime

Cloud VS. No Cloud

Cloud: 2.1 hours 4 times faster
No Cloud: 8 hours

Reported Events/Year

Cloud VS. No Cloud

Cloud: 2.5 Events
No Cloud: 3.1 Events

Data: Aberdeen Group 2010

Mostly we’ve been talking about backing up on-premise resources, but what if I’m already using a bunch of cloud services? Is there a role for a centralized cloud-based service to back up both premise and other cloud services?

We have been approached by companies who are using other cloud providers and they’ve asked if we can be the backup provider for that cloud data because they want to be assured they have their data in a safe and secure location regardless of what should happen. They look at us and say, “OK. You are BCRS. You’ve been around 50 years. You have over 160 resiliency centers around the world. You’re in 70-odd countries. I need a company that’s where I am, because data may not be able to leave the borders of certain countries. You’ve got the knowledge. You’ve done this before. Can you help me do it? If possible, we try to help to meet their needs.”
OK. So a company that wants to start evaluating the options here, where do they start? What questions should they ask themselves?

We actually have a consulting service we provide called SmartCloud Resiliency Transformation, where we sit down with the customer and say – OK, what have you done so far? Do you have any kind of a backup and recovery service today? What’s the current strategy and architecture look like? Have you evaluated your applications? What are your processes? What are your applications? What is your technology? We start there and then start to look at the potential cloud capabilities they could harness.

**Are there many instances where cloud doesn’t make sense?**

There are times when it may not make sense. If you’ve got some high transaction oriented applications that are not going to respond well to being in a cloud, it may not work. However, it still makes sense for, say, backing up data. Because all you’re doing is backing up the data and recovering it. So I’m hesitant to say there are specific examples that it won’t work until we take a look at it.

OK. Anything in closing?

Cloud is here to stay and more and more of our customers are going towards it. I think the adoption rate is increasing continuously, and I think that cloud for disaster recovery is a viable option for a lot of clients now.

**1) What is the most logical way to categorize the available solutions?**

Managed IT services providers often play an advisor role for Backup and Disaster Recovery or include it in their offering (Not recommended). So it's important to know the categories of solutions available, the best fit for your managed it services clients, and their costs.
• **Highly Automated:** Disaster Recovery and Business Continuity Solutions protect data centers and entire business infrastructures. *(VMware site recovery manager; vendor storage replication; snapshots; highly available virtualized infrastructures, etc.)* You usually see these in enterprise companies with large investments in IT Infrastructure, software and systems.

• **Partially Automated:** These solutions support local and remote-site backups, backup management and scheduling, incremental backups over the wire and partially automated recovery procedures. Either the vendor helps restore the applications and data, or the software solution has some built-in software recovery automation once the disaster event has passed. **Evault** and **AppAssure** are two examples.

• **Mostly Manual Backup Solutions:** These are local-storage, scheduled backups that mostly protect application data but require manual or bare-metal restores primarily. Recovery time objectives in such cases are a few days to weeks.

• **Consumer and low-end technologies:** Mozy, Carbonite, Dropbox and Box.net are among the providers in this category. While these aren’t true backup and disaster recovery options for businesses, they can be better than nothing, and they might evolve into more competitive solutions in the years to come.

2) **What are the strengths and weaknesses of each group?**

The costs are exponential when going from consumer to highly automated solutions. Backup and disaster recovery solutions are measured in terms of **recovery time objective** and **recovery point objective**.

• **Recovery Time Objective:** How long before you can get your systems back up and running? Think downtime.

• **Recovery Point Objective:** How much data did you lose when your system went down? If you take nightly backups, then it could be as high as 24 hours, if you take snapshots of your data every 15 minutes, then your maximum data loss would be 15 minutes.

The shorter you want your RTO and RPO, the more expensive the solution.

3) **What key questions should Managed IT Services providers think about when deciding which solution they will use?**

• What are the RTOs and RPOs that your business wants and needs?
• What solution meets those objectives?
• How much data do you really need to protect?
• Can the solution effectively handle that amount of data?
• If you have 10 terabytes but only 2TB is relevant then, maybe you can use a tiered backup and disaster recovery solution for the different types of data, based on their criticality.
4) What role, if any, should low-end solutions such as Carbonite, Box.com, or Mozy play in a managed IT services provider’s BDR strategy?

While having a backup solution is better than not having one, we don’t recommend using a consumer-grade solution in your business. We don’t support these solutions as a Backup or Disaster recovery solution for our clients.