# COMMON DISASTER RECOVERY PLAN MISCONCEPTIONS

## ENSURING YOUR DR PLAN DOES NOT LEAD TO DISASTER

Charles Street Solutions
28 Throgmorton Street
London, EC2N 2AN

Tel: +44 (0) 20 7256 5566
info@charlesstreet.com

## Common Disaster Recovery Plan Misconceptions

After being in the disaster recovery business for the last ten years, we have worked with thousands of companies on their disaster recovery projects and have built customer relationships with many of those. Helping so many customers has led to some unique perspectives and experience that readers should be aware of when developing disaster recovery plans that effectively minimize risk and ensure that business continues after a disaster strikes.

## Common Misconceptions

Outages do not discriminate. Not having had an outage for a year (or even ten years) does not mean you are any less vulnerable than anyone else. An outage may be nothing more than a wrinkle in your day or it can end your business in one fell swoop. One of the worst situations you can find yourself in is realizing you truly needed a DR plan when you did not have one.

But the good news is that we have also witnessed many companies experience what should have been a catastrophic outage without even skipping a beat. It all comes down to your plan and, more importantly, what assumptions your plan is making. People, timing, resource availability, and technology all play a part. Some of the assumptions are in your control, and some of them are not. Over the years, the companies that have been burned the most usually believed one of these four misconceptions regarding their DR plan:

- "I have a generator..."
- "We have not had an outage in a while, so other priorities come first..."
- "We have a BC/DR solution in place..."
- "We have a DR site in place..."

In our experience, these are the four primary misconceptions regarding a DR plan, and we will explore each one (and their corrective action) in more detail below. While we do give a few examples out of thousands of possible supporting stories, we chose to protect the names of the impacted. Being lambasted in the free press was enough for them.

## "I have a generator..."

If your primary concern is local availability, having a generator may have put your mind at ease. Unfortunately, it is not that easy and certainly not a DR plan. One of the central concepts within a DR plan is to remove as many single points of failure as possible. Single power grids, single sources of data, single connection points, all of these things will bite you when you least expect it. A generator gives you a secondary source of power, but we have all heard the stories – from the generator being out of gas or out of maintenance, to failures of generators and backup generators – which is exactly what happened

*Outages do not discriminate. Not having had an outage for a year (or even ten years) does not mean you are any less vulnerable than anyone else.*

in Northern Virginia in the summer.

**July: Severe thunderstorms hit Northern Virginia**

- 2.3 million people lost Emergency 911 service for 4 days
- Also led to more than 1 million customers & businesses left without power
- Reason: A backup power generator would not start

Note that not only did the first generator fail, the backup failed as well. The results were catastrophic. While many of the businesses in the region probably saw tremendous impact to their bottom line or reputation because of the outage, losing e911 services leads to an entirely different level of criticality. It is times like these that a tested DR plan, including back up communication and site strategies, prove invaluable.

**July: Storms cause power outages for a major Cloud provider**

- 2 major outages in 1 month
- Took down most of the top social websites that host in the platform
- Reason: One backup generator had a defective cooling fan and another was incorrectly configured

We all know this company and the services they provide. What most people did not know is how much of the web-based community of companies run on their cloud as well. Until July 2012 that is. This company not only had a backup generator in the affected location but they had a second backup as well! The first one was defective; the second one failed to start because of human error. This example also highlights that the cause of an outage can often only be part of the downtime equation. This is what we refer to as the anatomy of an outage. The first phase is determining there is an outage in the first place. This can take minutes, but can often take hours or days. The second phase is determining whether you can fix it quickly, or if you need to enact your failover plan. Finally, you have to recover in a way that ensures service is restored to your end users as quickly as possible. As if the outage was not enough, it took this particular company hours to recover the data and servers in what the company referred to as “a cascading series of errors”.

Having a generator alone is common DR plan misconception #1.

What both of these examples prove is that even the largest of companies, those that invest significant time and resources into continuity, can be caught in bad situations based on incorrect assumptions in DR/BC planning. Local availability plans only resolve half of the problem. If you are not able to fail over to another, separate location, communicate during the outage, and continue working from your DR site, you are not truly covered.

## “We have not had an outage in a while, other priorities come first...”

This is another common misconception and possibly the most dangerous. Those in the DR business immediately cringe upon hearing this because nothing is worse than seeing a customer realize DR should have been their priority when it is too late to do anything about it. Your business, your customers, and your image are all at stake. Investing in DR may not seem critical to many customers until it is too late, so it is definitely better to be proactive than reactive on this one. Let’s look at a couple examples of why.

**June/July: Major Online CRM provider experiences 2 outages in 2 weeks**

- Even with advanced separate instance redundancy, 7 instances went down
- Reasons: First outage caused by storage tier, second by power failure
- No major outages in 2 years prior

Don't fall into the same trap as in this example: separating your workload or installing basic redundancy does not constitute a full plan. Do not be fooled. You need contingency plans for failover, and a plan that communicates with and allows people to work during the time it takes to identify and resolve the issues. When it comes to outages, history does not often repeat itself. Each outage will uncover something new and different and there is hardly ever a situation or event you planned for. You can't let good fortune lull you to sleep and lead you to assume it won't happen to you. That is what this company thought and it happened twice in 2 weeks. Their rate of business guarantees there was significant impact to revenue, customer satisfaction, and reputation.

**June: One of the largest European financial institutions experiences 1st outage in years**

- Outage lasts over a week and affects 17m customers
- Reason: Issues during upgrade to batch processing software

This company found out what many other companies have and will find: the diagnosis of whether an issue has occurred, what its full impact is and whether you need to put your DR plan into action often takes up the majority of the overall outage time. In this example, the need to first establish when the outage had occurred took hours, creating a substantial backlog of delay in executing new batch processes. They simply couldn't keep up with events and their revenue and customers suffered dearly. Another example of the anatomy of an outage. Having a contingency plan in place does not help you in these times. You must have solutions that automate and triage this process to ensure the end impact is minimal.

These are only two examples of what hundreds, even thousands, of companies have experienced. Betting the future of your company on the hope that a significant outage will not strike your operations is risky at best and irresponsible at worst. Put a plan in place now, while you have the time to ensure and prove your plan will work when you need it.

## "We have a BC/DR solution in place..."

Having a solution in place is only a means to an end, not the end itself. Any solution can only provide full protection to your business if it implements a holistic DR plan that accounts for every area of your business, and the solution has been tested as far as is possible in planned and unplanned scenarios.

If your solution works but you have no way to communicate its implications for your end users, the business experiences the same impact as not having anything at all. Furthermore, if you invest and implement a DR solution without testing it, you will not find the inevitable glitches until it's too late! Also bear in mind that testing during a planned outage window only gets you half way there. A DR plan is not designed to remediate a planned, controlled situation. It is the unplanned and uncontrolled scenario that keeps you up at night. The times when resources are not available, when your team is worried more about their family than your servers, and the times when your back up tapes will not restore that truly prove your system and plan works. If all that takes too long and impacts your business too much to test, you have the wrong plan or the wrong solutions.

**July: Leading European Mobile company's systems fail**

- Outage impacts customers for more than 24 hours
- Reason: Experienced an unprecedented "fault" with a network system

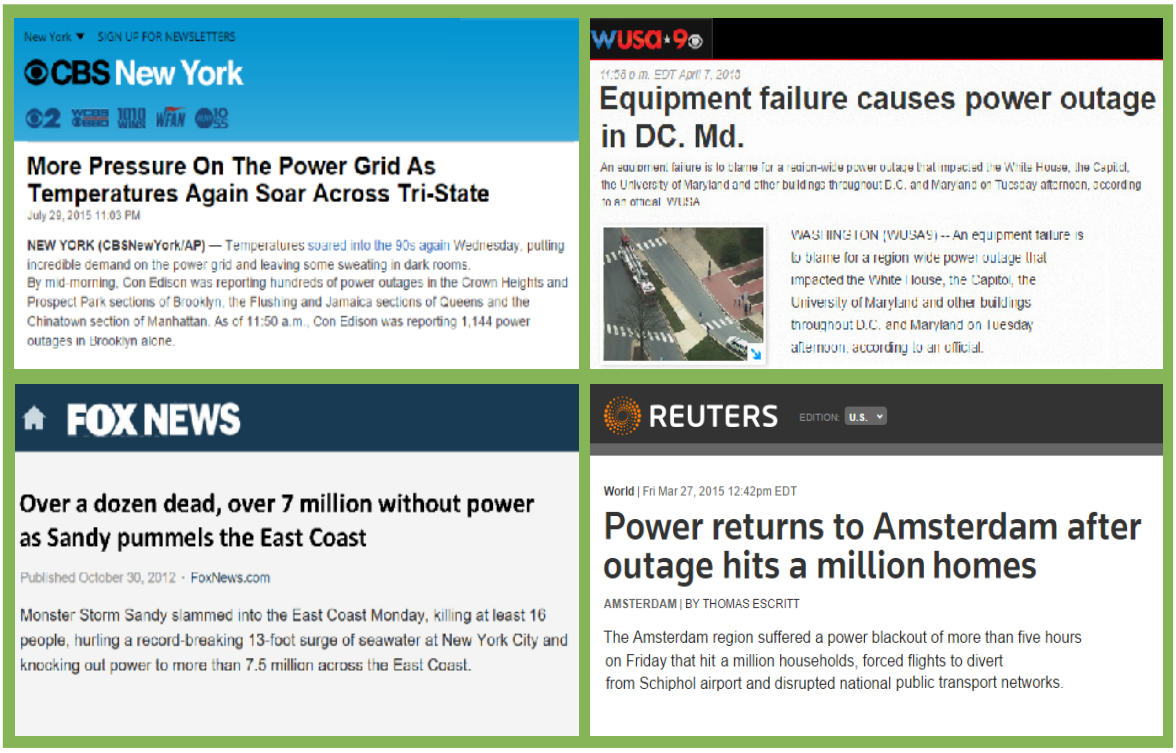
This mobile operator's customers were without service for 24 hours. The company's official statement: "Our ability to deliver a service to customers will rely on hundreds of different components, systems and applications working in harmony. This can make preventing these types of service disruptions difficult as well as finding the root cause time consuming."

Unprecedented is an often-used term in outage situations. Regardless of how complex your IT systems are, you owe it to your business and customers to have resiliency solutions in place, test often, and continually manage them closely. Your testing cannot just encompass planned scenarios. Automation, monitoring and failover can be invaluable in unplanned scenarios.

This misconception has impacted some of the biggest companies, those with the biggest budgets and BCP professionals on staff. Testing does not take a ton of complexity, budget and expertise in most cases. More often than not, these things only make recovery more difficult. You can have a plan and a solution set at any company size and any budget that is much simplified and effective. You just have to make sure you have accounted for all scenarios, covered both local availability and offsite recovery scenarios, and that you manage and test your plan often. Testing! Has your plan been tested? Is it battle ready?

## "We have a DR site in place…"

A separate DR location with local redundancy will only get you so far. One common problem arising from this misconception is that DR sites are often chosen for proximity and ease of access. If your DR site is on the same power grid or in the same region, it is possible for a single event to take out both sites. With the record-breaking heat, droughts, tornadoes, hurricanes and other disasters seen over the last few years, things like rolling black outs, brown outs, and power issues are becoming increasingly common.



What assumptions does your plan make regarding people and resources being available? How often do you test it? Does your DR site lie within the same power grid?

## Summary

What assumptions does your DR plan rely on? That people and resources will be available? That the data and applications will be as easily recoverable as they were during your test and/or proof of concept? That your generator will kick in? We all know that hope is not a strategy so why it is that many customers are willing to implement little more than a hope-based strategy when it comes to implementing and exercising their DR plans? The initial investment in a worldclass DR strategy may seem difficult to justify when you aren't in the middle of an outage, but you can bet the farm you would pay 10 times as much at 3am when the applications that run your business have been down for 24 hours and counting. It's as certain as death and taxes.

Our advice is to spend the time and money on a quality DR plan and supporting infrastructure now to mitigate your risk. And don't forget to test frequently to confirm your business will be protected when you need it most. If you have rested upon any of these misconceptions in the past, there is no better time than the present to ensure your business does not make the next headline.

## About Charles Street Solutions

Charles Street Solutions (CSS) is a dynamic & experienced technology services provider that has helped create, evolve & implement IT solutions & strategies to an extensive & reputable client base over the past 18-years. Through significant investments in UK data centres, ISO accreditations & in-house software development, our highly skilled teams are able to deliver unparalleled Private-secure hosting (aaS), Software Development solutions, traditional infrastructure projects, plus on going support & maintenance.

## About Neverfail® Solutions

Artisan Infrastructure's Neverfail Business Continuity Management solutions provide affordable software and services that deliver high availability, disaster recovery and data protection for critical applications. Neverfail's predictive approach protects businesses from planned maintenance and unplanned IT outages. Regardless of the nature of the problem, from a single system component failure to full site disaster, critical business applications will continue to run without disruption.

For more information on the Neverfail Business Continuity Management solutions contact Artisan Infrastructure at 512-600-4300 or visit www.neverfailgroup.com/products/neverfail-it-continuity-engine/.