EBOOK

FACTION®

# 6 MISTAKES YOU SHOULD AVOID MAKING IN YOUR DR STRATEGY

Disaster Recovery (DR) is best compared to an insurance policy. It can potentially be a big investment, but the moment DR is needed, you'll be relieved you have it. DR is a part of delivering Business Continuity (BC), the capability of an organization to continue delivery of products or services at acceptable pre-defined levels following a disruptive incident.

**Disruptive incidents can be anything that puts an organization's operations at risk, such as:**

- Loss of personnel
- Loss of facilities
- Loss of access to data or applications
- Equipment failure
- Natural disasters
- Cyberattacks (ransomware)

Typically, organizations create a plan and subsequent processes to ensure Business Continuity. Disaster Recovery needs to be a big part of this BC Planning because organizations need to be prepared for the worst. Even with a DR strategy in place, your organization might not be bulletproof. **Review our top 6 mistakes you might be making with your disaster recovery strategy.**

## According to the latest Forrester/ DRJ survey, one in three companies has declared a disaster during the past five years.

# 5 MAIN BENEFITS OF HAVING A DR STRATEGY IN PLACE

1. Mitigating risk such as snapshots or mirror copy failure & corruption, human error, hardware failure, or poorly documented configuration.
2. Minimizing downtime: aka keeping your business online!
3. Insuring against natural disasters by having geographic diversity: multiple copies of data in multiple geographies and cloud nodes.
4. Having the ability to withstand human error or physical impact on a production environment.
5. Limit effect on business or downstream customers.

## BUSINESS CASE

Can you make your business's technology resistant against a large-scale failure or outage today? How much downtime can you currently handle? How much will downtime cost you? In most cases, the cost of coming back from an outage without a DR strategy is much larger than the cost of the service itself.

Consider the airline outages that took place during the summer of 2016. Both Southwest and Delta experienced disruptions due to old technology failures. In August 2016, Delta grounded about 2,000 flights, and in July 2016 Southwest Airlines cancelled over 2,000 flights. These outages were caused by a combination of reservations systems dating back to the 1960's and not having invested in the proper DR strategies and services. Not only did these airlines suffer monetary losses, Delta's outage cost them about $150 million, while Southwest's was close to $82 million; their customers and reputations have suffered as well. Unfortunately, the outages they experienced could have been avoided, unlike weather delays.

**BOTH SOUTHWEST AND DELTA EXPERIENCED OUTAGES DUE TO OLD TECHNOLOGY FAILURES. IN AUGUST 2016, DELTA GROUNDED ABOUT 2,000 FLIGHTS AND IN JULY 2016 SOUTHWEST AIRLINES CANCELLED OVER 2,000 FLIGHTS.**

# AVOID MAKING THESE 6 COMMON MISTAKES WITH YOUR DR STRATEGY

## 1) Underestimating the impact of downtime and potential data loss to the business

Downtime is something that organizations need to be prepared to experience, which is why having a Disaster Recovery strategy in place is so important. It has become an accepted, virtually expected aspect of enterprise life. No organization is 100% safe from experiencing an outage, and the cost of downtime for each organization is different. For example, in 2011 major brands Bank of America, Verizon, and Netflix experienced devastating failures and outages. Bank of America's outage lasted 6 days and affected 29 million online customers; Verizon's outage lasted 24+ hours and customers across the US were affected; Netflix experienced an outage lasting 4-8 hours which affected 20,000,000 customers. It's important to take into account all of the aspects of a business that could be affected by an outage and how much it would cost you financially, down to the minute.

Downtime can also have a serious impact on company reputation and customer loyalty which can have a negative impact on organization's customer retention. It's also important to note that severe data loss can destroy an organization entirely. In 2014, SaaS provider Code Spaces failed to recover from being hacked and lost all of their data and backups in a matter of 12 hours.

## 2) Failing to properly identify the correct recovery time objective (RTO) and recovery point objective (RPO) requirements in your organization's DR strategy, and/or not updating these requirements as needs change in the future

Establishing initial RTO and RPO requirements is fundamental to your DR strategy. You need to be aware of the targeted amount of downtime as well as the maximum limit of data loss you can endure while an issue is being resolved. And what about the strategy you put into place 5 years ago? Does it line up with your current needs? Has your company grown? Do you have more employees than you did when you created your strategy? Ask yourself these questions and make sure your plan is up to date so situations can be addressed as quickly as possible and you can meet the RTO and RPO objectives laid out in your strategy.

## 3) Not modernizing applications and bringing all storage into a native Virtual Machine Disk (VMDK) framework to allow for a simplified replication strategy and maximum automation

Ensuring that your applications and storage systems are up to date can greatly impact how an organization comes back from an outage. Most modern BC/DR software solutions rely on data being in VMDK framework. This will increase accessibility, scalability, and functionality of your data while minimizing costs, complexity, and failure of your DR solution.

## 4) Not having a reference guide on hand of failover and runbook procedures

By definition, a runbook is a compilation of routine procedures and operations that the system administrator or operator carries out. Having a step-by-step reference guide available during an outage can prove to be extremely useful when determining the most effective response. This runbook will serve as a strategy to identify next steps toward recovery in the most effective way when disaster strikes.

## 5) Not aligning RTO and Workload requirements to the best cloud product

Cloud-based disaster recovery, or Disaster Recovery as a Service (DRaaS) is a DR method that has gained traction in recent years. It's important to make sure that your cloud provider understands your needs as an organization and aligns their product set to meet the time requirement and deliver the best price point possible. Your RTO (recovery time objective) must be made clear so that you are both working towards the same goal. Prioritizing applications into groups based on RTO is an effective way to both create a priority level within the runbook and a within the budget. At the end of the day, protecting your data comes at a cost, make sure that aligns with the value of what you are protecting.

## 6) Not testing your DR strategy regularly & completely

If an organization fails to completely test their DR solution, there is no way to know if it will actually work. Even the most carefully crafted plan can end up useless if it doesn't function properly when you need it or only recovers a fraction of the data lost. Full-scale tests can be costly and timely, but they are critical for long term success of the DR strategy. Many companies do a small test or one that is limited in scope and never uncover major flaws in their plan. Doing full end-to-end testing is the only way to ensure that you are ready and capable to execute a recovery in the event of a disaster.

Making these 6 mistakes can significantly impact your organization should a disaster occur. Take a look at your Disaster Recovery Strategy to see if you can identify changes that need to be made to ensure your organization can successfully recover from an outage.