

A large graphic of a water droplet splashing into a pool of water, creating concentric ripples. The background is a gradient of blue and white. The word 'Save' is written in a serif font with a horizontal line under the 'S' in a light grey box in the top left corner.

Save



Ensuring Effective Disaster Recovery

While most companies have some sort of a plan to protect (i.e., back up) their data, amazingly few companies include disaster recovery planning as part of their data protection strategy. Disaster planning in the IT organization is like buying insurance ... it's easy to think "it'll never happen to me" but if it ever does and you're not protected, the end results can be catastrophic.

Why is Having A Disaster Recovery Plan Important?

Most people associate "disaster planning" with natural disasters such as fire, flood, earthquake, etc. While these disasters can and do occur, they occur infrequently. Other events that put your corporate data at risk occur somewhat more frequently—data centers can lose services (power) or you can lose access to your data center. But there are much more regular events, such as disgruntled employees or people with malicious intent, that put your data at risk—practically on a daily basis.

Disaster recovery is all about making sure you have duplicate copies of your mission-critical data stored at a secure, offsite location. In some cases, it depends on a responsible management team to understand the importance of and then execute disaster recovery plans. In other cases, the need for an effective disaster recovery plan is mandated by federal regulations.

If you are managing periodic backups, then you've already determined that data is critical to your business operations. But if you've not closed the loop and implemented an effective disaster recovery plan, your data is still at risk of being temporarily or permanently unavailable.

Disaster Recovery Planning Affects Business Continuity

Think about the worst case scenario. If you lost access to your data, how long could you afford to be without that data? Chances are if you lost access to customer data, inventory information, financial database information, emails or electronic transactions your business would come to a screeching halt. How long can your business survive in such a situation?

The #1 priority in disaster recovery planning is to determine how long your business can survive with data loss. Think about how valuable the data is and how long it will take to get it back. Think about how much data you have that's critical to your business continuity. Once you've identified these aspects, you can begin putting together an effective disaster recovery plan.

Disaster Recovery Planning Begins with You

If you're responsible for protecting your company's data, the most important thing you can do is put a plan in place that creates separate copies of your data at different locations. Because the importance of that data can vary, and your regulatory compliance factors and service level agreements can vary, no organization can effectively protect their data with just a single solution. So focus on those solutions that will minimize risk and reduce cost in all aspects of your data protection hierarchy.

Tiered Data Protection Appliances from Overland Storage® offer midrange and distributed enterprises the ability to effectively protect their data in the event of a disaster. Overland Storage high performance RAID arrays, advanced disk-based virtual tape libraries and best-in-class automated tape libraries enable movement of data to secure, remote disaster recovery sites while ensuring that the data can be quickly retrieved when needed. Whether it's the risk of natural disasters or man-made events, Overland Storage ensures that information is constantly protected, readily available, and always there.

