Avoiding Disaster Recovery Epic Fails

By Dr. Mark Campbell, Chief Strategy & Technology Officer, Unitrends

Most disaster recovery (DR) articles focus on convincing readers that the risk of a business altering disaster is real, and as such, they should buy a set of products and services to mitigate that risk. But, if you're reading this, I know you already understand the importance of DR, and so my focus will be a little bit different. This article will explore various causes of DR epic fails – ranging from traditional issues, such as backup and replication malfunctions and a lack of planning, to new challenges, such as assuming homogeneity.

According to the National Archives and Records Administration, 93 percent of all businesses that lost their data center for 10 days went bankrupt within one year. Armed with a few key best practices, you can eliminate this risk by building an effective DR strategy that will protect your corporate data and your job.

What Causes DR Epic Fails?

Before we begin, let me mention that I'm going to resist the siren lure of the word "cloud". The cloudwashing of DR has reached such a fever pitch that it's almost impossible to read about the topic these days without feeling as if the cloud is the single most important concept since either fire or the wheel. And yet, successful and unsuccessful DR implementations have been occurring long before the advent of cloud computing and will of course continue without it. Don't get me wrong, the cloud is an important implementation vehicle for DR – but it doesn't ensure successful recovery from disasters. The foundation of a strong DR plan revolves around a few basic principles that don't involve the cloud. Let's take a look at the most common reasons DR strategies fail and best practices to overcome these challenges.

Reason One: Malfunctioning backup technology.

Most people will tell you that planning is the most important thing you can do to avoid a DR failure. But they are wrong. Planning actually falls second in the ranking order, preceded only by the backup technology you have in place. Why? All the planning in the world will not secure your data if the technology fails.

Backups and replication are the foundation of a modern DR plan, and as such, it's critical to ensure that the technology is working as it should – e.g., backups are automatic and reliable, the integrity of your data is upheld through inline and offline validation, auditing is automated via failover virtualization and backups are replicated successfully to a secondary location. In simple terms, make sure your data is actually being backed up and replicated to an offsite location. This process provides an added layer of redundancy so that if your primary location's data center goes down, information is still accessible via the secondary site, and business operations can proceed unaffected.

1 National Archives and Records Administration

2 Urban Dictionary

Archiving is also an important consideration in DR and can be used to either replace or supplement replication. Archiving can be performed on a disk-to-disk-to-any (D2D2x) basis, where the archive target can be a rotational disk, rotational tape, fixed NAS or fixed SAN. Archiving is a great way to augment your WAN if bandwidth is limited. But, keep in mind that rotational archiving is limited in some disaster scenarios. For example, I knew an IT administrator who used rotational archiving but couldn't switch the archive target in a disaster because flooding prevented him from physically driving to the office.

Another important consideration to keep top of mind is to never neglect your systems. Data backup is only effective if you have available systems and infrastructure upon which to access it. Consider techniques such as dissimilar bare metal recovery and virtualized "instant recovery" to ensure your data and systems – and your business – will be back up and running quickly after a disaster strikes.

Reason Two: Neglecting to plan.

If backup technology is the solid rock upon which you build your DR strategy, then planning is the accompanying foundation. Proper DR planning means actually writing up a document that is broad in scope and covers step-by-step guidelines on what to do in the event of a disaster. Strong DR plans focus on three primary areas:

- People: Identify key operational personnel and provide them with the ability to work remotely or at a secondary location when a disaster strikes. This means giving them direct access – regardless of their location – to the recovery systems, data and other resources they need to maintain business operations. It's also important to set up an alternate form of communication (e.g., employees' cell phones) in the event that your organization's primary communications infrastructure goes down (e.g., corporate email or phone systems).

- Infrastructure: Identify key operational infrastructure – those parts of your infrastructure without which your business can't operate – and make sure they are protected. It is incredibly important to remember that the reason that you want your IT infrastructure to successfully survive a disaster is so that your most important assets – your staff – can use your systems and your data after the disaster to continue to drive revenue and profitability for your company.

- Processes: Identify key operational processes – step-by-step guidelines for who does what in the event of a disruption – and make sure employees are aware of and have practiced their role. Having cross-organizational buy-in is an extremely important piece of the puzzle. Remember to consider every process that is critical to the daily operations of your business. Don't just focus on IT processes.

Your DR plan, as well as your data protection solutions, should also meet your company's Recovery Point Objectives (RPOs) – or the maximum amount of data (in terms of time) that you can afford to lose – and Recovery Time Objectives (RTOs) – or the maximum amount of time that you can afford to be without your data and systems. The best DR plans are based on how much data is being recovered and how quickly that information needs to be brought online.

Reason Three: Failing to test, test and test again.

Companies typically make one of two fundamental mistakes when it comes to DR testing: They fail to test plans and processes on a consistent basis or fail to test real-world DR scenarios. Not performing DR testing on a consistent basis is a major issue for administrators because of the ongoing evolution of IT infrastructure. There is often a divergence that is difficult to capture that is related to, but not wholly reflected by, the assumption of heterogeneity. The cure is thorough, iterative DR testing that is done on a consistent schedule that allows it to be adopted as yet another standard business practice. The change rate of your data is a good benchmark to determine how frequently to test your disaster recovery plan.

Real-world DR testing means considering various disaster scenarios and evaluating how DR processes may change as a result. For example, earlier, I mentioned the IT administrator who used rotational archiving in his DR strategy, but didn't take into account that, depending on the disaster, he may not be able to physically rotate the media. Had he tested his DR plan with a variety of disaster scenarios in mind, he would have realized his mistake and put different processes in place for different types of disasters.

I highly recommend that anyone responsible for DR read the works of Nassim Nicholas Taleb. Nassim has written extensively about something he calls the "Black Swan." From Wikipedia:

> *"The **black swan theory** or **theory of black swan events** is a metaphor that describes an event that is a surprise (to the observer), has a major effect, and after the fact is often inappropriately rationalized with the benefit of hindsight."*

From a DR perspective, this would be like deciding that your only disaster risk comes from flooding, and then locating your business above the 100-year flood plan with no other means of disaster prevention – which leaves you at risk to suffer from other types of disasters.

Creating an effective DR plan isn't just about grinding through apparently endless processes and details; it also requires the creativity to think outside the box and consider a variety of different disasters and resulting DR consequences. In other words, seriously consider the disaster scenarios that you deem impossible in addition to those you think most probable – because, in reality, you just never know.

Reason Four: Assuming homogeneity.

Simplifying your IT infrastructure is always a good thing – until it isn't. Let me explain. In order to maximize ROI, it's important to maintain flexibility so that IT remains responsive and agile to the changing needs of its users and to the evolving technology and vendor landscape.

To take the most common example, avoiding single vendor lock-in is critical to both the technical and financial success of modern IT. DR failures often occur because administrators support only a single technology in their planning. For example, they'll support storage technologies such as SAN or NAS, but ignore direct attached storage; embrace virtualization, but ignore physical servers; or support physical appliances, but fail to consider the need to restore between different models and generations of servers. Implementing a DR plan and accompanying technology that embraces heterogeneity and adapts to agile IT environments will be the most effective when you need them most.

3 The Black Swan: Second Edition: The Impact of the Highly Improbable, Nassim Nicholas Taleb. www.unitrends.com

Conclusion

To summarize, implementing an effective DR strategy doesn't have to be difficult or consume multitudes of IT resources. Functional backup technology, detailed DR plans, continuous testing and heterogeneity is the core foundation that will prevent disaster failures and propel you to DR success.

About the Author: *Dr. Mark Campbell is the chief strategy and technology officer at Unitrends. Prior to joining Unitrends, Mark co-founded mindAmp Corporation, which provided high-technology business and software development consulting. He has also worked as the senior vice president and general manager of the systems management business at Legent Corporation, as well as vice president and general manager of the enterprise systems business at AT&T and NCR Corporation.*

Visit Unitrends for additional information
http://www.unitrends.com/features/disaster-recovery.html

UNITRENDS

7 Technology Circle Suite 100
Columbia, SC 29203