arcserve®

WHITE PAPER

Top 10 Gotchas of Disaster Recovery and Business Continuity Planning

Business continuity — the planning, preparation, and implementation of more resilient business systems in anticipation of unscheduled downtime — is often thought of as an IT problem, and most organizations leave it to the IT department to provide a fix. This invariably leads to the deployment of a wide range of tactical solutions, with no overriding strategy providing guidance. In reality, as the term implies, business continuity is a business problem, and it requires a business approach to fix it.

How would you know if your current business continuity plan is solid? Here is a quick checklist for you.

- Does your plan require significant manual intervention?
- Does your plan accept loss of data beyond a few seconds for critical systems?
- Does your plan restore access to critical systems in more than an hour?
- Does your plan depend on 30-year old backup and recovery technology?

If your answer is yes to any of the above questions, the chances are you are exposed to data loss and business downtime.

Everyone talks about how to do disaster recovery the right way, but isn't it just as helpful to take a look at the pitfalls that await you if you do it wrong? That's why we've prepared the top 10 gotchas to assist you with your planning and decision making.

1. It's About the Business, Not Technology!

It's important to remember that disaster recovery is about satisfying a business need and must be driven by business requirements. Before trying to work out how to implement disaster recovery, you need to spend time thinking about Why. Talk to business leaders to understand their priorities. Whether it's done through email or face-to-face discussions, the point is that you won't know what systems are the most important unless you ask business users. Understanding the needs of the organization will let you set priorities that dictate your technology choices.

2. It's a Catastrophe, or Maybe Not

When you think about disaster recovery, you probably picture hurricanes, floods, terrorist attacks, and the like; not a software upgrade gone wrong or a hardware error on a critical piece of networking equipment. Planning for the worst-case scenario and being tripped up by trivial day-to-day errors is very common. Your planning has to take into account all eventualities, from the ordinary to the cataclysmic.

3. How Can You Assign Budget Without Knowing The Cost of Downtime?

In most cases organizations assign a dollar value for disaster recovery planning before determining the financial risk of downtime and data loss to the business. Unless you can quantify how much you can lose from an

outage to critical systems, it will be difficult to state how much you can spend to avoid these losses. This means assessing the financial cost of downtime before allocating a budget. Don't forget to include regulatory compliance in your cost of downtime calculations. There are often financial penalties for unmet legal obligations.

4. It's About Measuring Risk

Exactly what events classify as a disaster can change from organization to organization, and even from department to department. Some events – earthquakes, for example – are potentially so catastrophic that it is obvious the organization must protect itself. Other events may be common – such as failed network hardware – yet have an outsized financial impact. When thinking about disaster recovery, it is essential to ask: What are we trying to protect ourselves from? Don't overlook the commonplace. Small losses from common problems mount up quickly.

5. Do You Have A Plan?

If your disaster recovery plan is a Post-it note on the backup tapes under your system admin's bed, you're in trouble. As crazy as it sounds, a surprising number of organizations don't have a disaster recovery plan. It is essential that you develop a formal document detailing all applications, hardware, facilities, service providers, personnel and priorities, and you must obtain buy-in to the document from all the stakeholders in the organization. The plan must represent all functional areas and offer clear guidance on what happens before, during and after a disaster.

6. We've Got A Plan, But We Didn't Test It

Maintaining a disaster recovery plan is only helpful if it works. The only way to ensure your plan works is to test it. Testing the plan under simulated disaster conditions is essential, but it can also be challenging. Performing disaster recovery testing is expensive and takes time and resources away from day-to-day operations. However, unless recovery is fully tested at the application level, you will inevitably encounter difficulties during a real-world disaster. Look for data protection solutions that help you create environments for non-disruptive testing of your disaster recovery plan.

7. Who is Responsible and for What?

A real-life disaster event will be chaotic and confusing. If the key staff does not understand their disaster recovery responsibilities, the recovery process will be long and fraught with problems. Your disaster recovery plan must clearly state the roles and responsibilities of everyone involved, including what to do if the key personnel are not available. These people should also be involved in testing your recovery plan.

8. Recovery Point What? Recovery Time Who?

Two metrics are used to record an application's tolerance of downtime and data loss: recovery point objective (RPO) and recovery time objective (RTO). RPO is a measure of data loss. The larger the RPO, the more data loss each application can tolerate before it becomes a problem for the business. Think of it as the point in time that you can successfully recover data up to. All data between that point and the time of the disaster is gone. RTO is a measure of recovery time. The smaller the RTO, the faster you have to work to get the application back online before the organization starts to suffer significant losses. If you don't know the RPO and RTO of each application, you're in the dark when it comes to disaster recovery. RPT and RTO allow you to define levels of service that you can deliver against.

9. Recovery Will Take Longer Than You Think

Understanding how long it will take to recover key business systems is essential. Even if you can access offsite backup copies, there is no guarantee that you can recover applications in a timely manner. Can you restore data and rebuild application systems fast enough to satisfy business users? Do you have the bandwidth to recover data from a cloud service provider? Understanding how long it takes to recover applications and the effect of downtime on the business, may prompt you to make different technology choices.

10. Going Home

Going back home after failing over to a disaster site is an often overlooked component of disaster recovery planning. It's easy to see why. When we think of disaster, our minds focus solely on protecting valuable assets Little thought is given to what happens to those assets after the disaster event has passed. The ability to failback to production systems is every bit as important as the ability to failover. Unless carefully planned, a backup data center is unlikely to have the same capacity or performance as the production site. Without a failback plan, you may perform a successful initial failover and then see losses mount as your business limps along for weeks operating from an inadequately provisioned backup site.

Downtime and data loss are a fact of life for businesses that rely on IT. Offsetting this risk with the right technology must be a consideration at the earliest stages of the software development and product deployment lifecycles. Understanding the protection level demanded by each application lets you allocate the appropriate resources. By the time an application is in production use by business users, its RPO and RTO must be clearly identified and the appropriate business continuity solutions implemented to provide assured recovery in the event of an outage.

Arcserve® Unified Data Protection

Arcserve has been providing zero downtime protection to organizations around the globe for over 20 years. Now, Arcserve Unified Data Protection (UDP) delivers a one-stop-shop for all of your data protection and high availability needs. With centralized control, Arcserve UDP unifies backup, snapshot, replication and deduplication for your virtual, physical, on-premise and cloud-resident application assets. Arcserve UDP Assured Recovery™ provides a comprehensive real-time disaster preparedness test process for non-disruptive validation of business continuity plans. To find out more, please go to **www.arcserve.com**.

arcserve®
assured recovery™