

A Practical Guide to Business Continuity

Executive Summary

One of the most important, but seemingly most overlooked, aspects of a complete data protection solution is a Business Continuity plan. The list of why's are endless, and common: the cost of implementing a plan seems expensive, the planning itself takes more time and follow through than budgets and clients allow for and finally, the question always remains, when will you actually use it?

Too often, Business Continuity (BC) and Disaster Recovery (DR) planning fall by the wayside for these exact reasons. However, business continuity is the most important planning you can do. After all, what happens when you cannot get to your critical data? The trick is to use a little common sense and whittle the job down to practical terms that can be implemented, budgeted, and executed in a timely manner. The goal is to never have to use BC and DR plans—other than verify that they work—but to have just enough insurance and resources to keep things going without hurting the operations of the business. The following whitepaper is a practical guide to building an affordable, but comprehensive, business continuity plan that is part of an end-to-end data protection solution.

Defining Business Continuity and Disaster Recovery

Business Continuity

Business Continuity is the ability to keep vital business operations running in the event of failure in the existing infrastructure. These failures can include power failures, application errors, network failures, data integrity issues, human error or any other issue where the majority of the infrastructure is still in place, but operations are halted and need to resume.

Disaster Recovery

Disaster Recovery is when the infrastructure is significantly impacted and no longer available, impacting Business Continuity. This is most often a major natural disaster or other “act of God.” The number one requirement in DR is that the data is protected off-site. Data is the only thing truly unique. It is the only thing that cannot be readily replaced.

Do not Plan for the Perfect Storm

We have all heard the “perfect storm” scenarios where a random series of events has led to a seemingly inconceivable disaster. Often, papers on BC and DR site these major disasters as the reason for planning and funding these programs, when the reality is that they do not happen often and when they do it is almost impossible to plan for every imaginable disaster. The truth is, most BC/DR incidents are not full-blown natural disasters. According to Strategic Research Corp., the primary causes of BC/DR incidents are:

- 44% Hardware—A system component fails (can include servers, switches, disk drives, RAID controllers and/or another core piece of infrastructure) causing a loss of services.
- 32% Human Error—The primary cause of human error is either a mistake in a configuration setting, or issuing the wrong command on a production system. This can usually be prevented with testing, but often these changes are being made on-the-fly and time does not allow for adequate testing. This happens frequently after hardware replacement.
- 14% Software and Firmware Errors—These failures are often related to operating systems hanging, driver incompatibilities and the introduction of new applications to servers that contend for resources.
- 7% Virus/Security Breach—The reality is that malicious attacks happen, often as system users download files from unsecured sites. These activities cause real problems that require a solid recovery plan. This is where the ability to maintain an RPO (Recovery Point Objective) is vital to bring systems back to the time before the attack without any data corruption.
- 3% Natural Disaster—Natural disasters are often cited as a leading reason for BC and DR planning but they represent a relatively small percentage of actual BC and DR events.

Beyond the research related to the leading causes of BC and DR events, a company needs to focus on having a plan and an agreed-upon response to his company's top concerns. It is recommend building “what-if” scenarios and testing them to see what you have, what you need, and where the gaps exist. For example:

- What if we have lost our RAID array?
- What if we have lost our primary network switch?
- What if we have lost our tape library or Virtual Tape Library?
- What if we have corrupted our finance, web, or email application server?
- What if we have lost all power to the data center?
- What if we only have our backup tapes and all the hardware is gone... how do we recover?
- Regulatory SLAs for data protection are...?
- What if we need to restore all data in (XX) minutes or hours?

Like most design efforts, greater value is achieved from time invested up front. The next section outlines a model to build a BC/DR plan.

Key Points of a BC and DR Plan

To state the obvious, the most important thing is to have a plan and to have set the proper expectations about the effectiveness of the plan based on business and technical resources. Next, is to conduct an initial test of the plan, review it on a regular basis, and conduct spot tests on a random basis. The base process for BC and DR plans is simple:

Step 1: Define and Assess

What are the priorities of your organization? Understand what issues you face from business, contractual and regulatory perspectives, and set these as a minimum. Define how long your business can be without computer services. Once you have defined what needs to be done (key applications and services), and how long you have to do it, then the process becomes more manageable, budget-friendly and executable.

Typically, the top items for small business are:

- Keep Revenue Flowing
- Keep Communications Up (Email, IM, Phones)
- Keep Customers Engaged and Happy (Web Site, Service and Shipping)
- Track the Transactions (Billing and Accounting)

Step 2: Research and Recruit

Now that you know what needs to be protected, talk to suppliers and partners to find out what tools and options are available, then build a set of key data (equipment, services, budget) to help get ready for designing a solution. This is a topic that has been well documented by other companies and information on best practices is easily accessible online.

Step 3: Design

Hit the whiteboard and map things out! Document the design, then outline the testing and ongoing monitoring of the plan and tools. This is where the greatest cost—and your greatest success—will come from. At this point, you should bring in not only technical resources, but also business partners to test the impact and implications of the proposed plan.

Step 4: Implement

Now that you have a plan, process and budget, get the equipment and start implementing the BC/DR changes. This will almost always be a phased approach designed to reduce impact on production systems. Implementation should be based on business risk reduction, budget realities, and technical capabilities.

Step 5: Validate

Once you have the first four steps implemented, we suggest two ways of validating the BC/DR plan. The first is from Jon Toigo, CEO of the Data Management Institute. He suggests walking around your building and placing colored Post-it® notes on hardware throughout the building.

For example, a yellow Post-it would signify a hardware failure, while a blue Post-it would signify the application running on that device failed. Then gather your team and workshop each step of the solution, ensuring that the team clearly understands what needs to be done in the Post-it scenario. The second way of validating your BC plan is to actually take your systems down, and then clearly document, step-by-step, the process to rebuild the application, the network, or storage to an operational state. This way, you clearly understand how it affects users, the business and your customers.

Step 6: Maintain

Make sure you have the tools and software in place to monitor the equipment and networks you need available for your BC and DR plans. Ensure that you have budgeted for on-site spares or the proper service contracts.

Building the Plan and a BC/DR Score Card

It is easy to over-build a BC/DR plan, so here are a few simple tools to help you work through the key “what-ifs” and to help with budget justification. The first tool is the BC/DR scorecard that will provide you with a checklist to help analyze your needs.

The second tool is a BC/DR justification tool. One significant challenge for most BC and DR programs is determining the budget. In a recent report from Network World, “A conservative estimate from Gartner pegs the hourly cost of downtime for computer networks at \$42,000, so a company that suffers from an average downtime of 175 hours per year can lose more than \$7 million per year.” Obviously, this estimate is based on a larger organization, but the cost of downtime is not just a single number, it varies by applications and company size.

Building the Plan and a BC/DR Score Card

In a recent paper from ESG (Enterprise Strategy Group), they polled companies using disk-based backup to meet specific recovery timeframes for key applications. 69 percent of respondents had recovery periods of less than two hours—mere minutes to recover data for key transactional systems such as CRM, ERP, ecommerce and other mission-critical applications. The storage part of BC and DR planning needs to provide three types of recovery:

- **RTO (Recovery Time Objective)** defined as how quickly you can find, access and retrieve required information.
- **RPO (Recovery Point Objective)** defined as the point-in-time (PIT) the business needs to be able to recover... or the ability to roll back to a specific moment in time.
- **RPO** is a measure of the tolerance for data loss, in other words, how many transactions or hours of work the company can tolerate losing.
- **RG0 (Recovery Granularity Objective)** this is how granular the storage architecture recovery needs to be: file level, block level or at a transaction level.

A combination of hardware and software is required to meet each of these recovery objectives.

Each combination enables a company to meet the three dimensions of recovery, and provide the right solution. Disk-based backup is at the core of all these plans, in order to provide high-speed access to data and provide instantaneous recovery of data.

Storage Networking and Consolidation:

- **Single Storage Protection Policy**—Consolidated storage is the key to building a solid and sustainable BC and DR plan. It enables a company to build a single set of data protection policies and have them executed in a unified fashion. When the storage is centralized it is easier to support with a single plan, it is easier to manage and easier to validate BC and DR plans.
- **Rapid Restore** — Storage networking, combined with disk-based backup, is vital for business-critical applications such as transaction systems, web sites and email.
- **Off-site DR**—Again, the combination of storage networking and disk-based backup are vital to provide off-site DR and BC capabilities. The limited bandwidth of telecommunication lines require high performance and low latency storage for maximizing the use of expensive Telco lines and to ensure synchronous communications.
- **Regulatory Requirements**—Almost every business has regulatory requirements related to data protection, security, and application availability. For any public company and many companies that supply government agencies, BC and DR plans are requirements. The partnership of storage networking and storage consolidation provides the tools required to share and replicate data locally and over distances.

Disk-Based Backup Solutions

There are several options for disk-based backup to meet recovery requirements for RTO, RPO, and RG0. As you would expect, the cost of these solutions is directly proportional to RTO, RPO and RG0 access time objectives.

Summary

Business continuity is a big issue for petroleum marketers. Like most things, a little planning and preparation can go a long way in making a BC or DR program successful. The best way to proceed is to break the problem down into smaller pieces so they can be more easily managed.