

A Breece Hill White Paper



Key Considerations in Planning a Data Protection Solution

September 2006

By Breece Hill, LLC

246 S. Taylor Avenue
Louisville, CO 80027
Tel 1.800.941.0550
www.breecehill.com

Abstract

The primary concern of nearly every business owner is growing the business, yet key business drivers continue to prevent organizations from achieving optimal results. Companies are faced with a myriad of issues that impact business — from hackers and identity theft to rising insurance and infrastructure costs. These problems are not unique or unsolvable, just numerous. When dealing with these issues, we sometimes throw caution to the wind. While this may sometimes be the right strategy for winning new customers; it is not the right strategy for protecting your business.

Everyone is vulnerable to the catastrophic effects of lost data. A company's customer database, the last few months of sales records, shipping invoices, and purchase requests are just a few of the things that need to be protected. This paper discusses some of the challenges and requirements of protecting your company's assets and a unique approach that emphasizes easy and effective data recovery.

Understanding the Issues

Uninterrupted business operation is rapidly becoming the single most daunting task facing businesses today. *Disaster Recovery Journal* concluded that for each hour of downtime, the average hourly revenue loss is about \$78,000. *The Wall Street Journal* states that a company experiencing a downtime of more than 10 days will never fully recover financially and, 43% of businesses sustaining a major disaster never reopen. Hours of downtime can be costly; days of downtime can be catastrophic.

An effective data protection strategy is not built on hope. The process is multi-faceted and involves both Business Continuity and Disaster Recovery planning. Business Continuity identifies the activities needed to ensure that it continues to operate in the event of catastrophic loss or corruption. With a good Business Continuity plan, critical applications and data will be available no matter what type of disruption has occurred. Disaster Recovery forces a company to understand what is needed to ensure that data and systems can be restored to a usable and predictable state. To implement an effective, comprehensive solution, planning ahead is key — simply reacting to unfamiliar problems only results in unpredictable and costly mistakes.

What's the difference?

Business Continuity	Describes the processes and procedures an organization puts in place to ensure that essential functions can continue during and after a disaster. Business continuance planning seeks to prevent interruption of mission-critical services, and to reestablish full functioning as swiftly and smoothly as possible.
Disaster Recovery	A disaster recovery plan consists of the precautions taken so that the effects of a disaster will be minimized, and the organization will be able to either maintain or quickly resume mission-critical functions. Typically, disaster recovery planning involves an analysis of business processes and continuity needs; it may also include a significant focus on disaster prevention.

A great deal of time, money and effort has been spent defining terms such as Recovery Time Objectives (RTO), Recovery Point Objectives (RPO), and Data Protection Windows (DPW). These efforts extend beyond "backup" strategies to include "disaster recovery" initiatives. Businesses have discovered that it is not enough to focus solely on backup; understanding the aspects of recovery is imperative for business survival.

For small and mid-sized companies (SMB), a comprehensive plan was previously unobtainable because of the high cost. Today, multiple tiered storage, which was typically only available to enterprise level businesses with large budgets, is now a reality for small and mid-sized businesses. With hardware prices falling 20-30 percent each year, the infrastructure costs are less expensive than the value of data being stored. With lower cost alternatives available, companies of all sizes can implement a solution to ensure their business critical data is protected.

Advance planning and the selection of the right solution are your best bet. Knowing that you have taken the time to understand a few key considerations will assist in executing an informed decision that best suits your business needs.

7 Essential Considerations to Protect Your Business

You can't just think about business that will be lost due to a catastrophic failure or loss of data. In today's world, you need to think about loss of productivity, potential government fines for not being able to produce documents and even law suits because of undelivered products or services. To ensure you aren't caught in the middle of a disaster, consider the following seven key aspects:

Consideration	Questions to Ask
Completeness	<ul style="list-style-type: none"> • What's your laptop worth? • What about the laptops of your entire sales organization? • What if they can't get to their data?
Security	<ul style="list-style-type: none"> • Can someone get to your company secrets? • What if there is a security breach?
Recovery Objectives	<ul style="list-style-type: none"> • Is your backed up data protected against viruses or data corruption? • How often do you check to ensure you have "good" data?
Open Files	<ul style="list-style-type: none"> • How are you protecting your system and configuration files? • Do you have to pay more to protect them?
Verification	<ul style="list-style-type: none"> • How do you know your backup is complete? • Do you have to completely restart backup operations during a failure, wasting time and money?
Bare Metal Recovery	<ul style="list-style-type: none"> • Can you recover even if your computer has died?
Database and Mail Servers	<ul style="list-style-type: none"> • How do you backup individual mailboxes and messages? • Can you afford to lose the information?

Completeness

What are the laptops in your organization worth? We aren't talking about the hardware either. While it is relatively easy to quantify the cost associated with the loss of data from a server, it is also important to consider the loss of data on unprotected laptops and desktops. Complete data protection covers all computers. Do you know how much of your critical data is

located on each? Because of the mobile nature of laptops, your IT staff may need to create a separate protection and recovery plan for information on these systems.

For all systems, consider how frequently the data is updated. Unlimited clients, auto-backup and auto-discovery should be standard features required in your solution. Support of unlimited clients ensures all of your data is protected. Auto-backup protects these systems and minimizes the level of IT intervention. For example, once a laptop is added to your environment the software should allow for an opportunistic backup when the laptop is available. Other options to consider include "Smart Backups" for timely updates of data. Look for a system that helps evaluate, differentiate, and prioritize backup of various systems based on your business requirements.

Security

Confidentiality and protection are two critical aspects to data security. Data encryption provides a simple cost effective means for "reasonable care" of sensitive and confidential information. Your solution should protect the data from both internal and external breach points. It is necessary to select a system that provides multiple levels of security; passwords meet only minimum requirements.

Full-featured functionality includes Data Encryption Standard (DES) as well as implementations of the Advanced Encryption Standards (AES), using 128-bit and 256-bit technologies. All solutions that promote removable media should include encryption for data stored on media. While all encryption systems necessitate the understanding of "key management," look for one where management is integral to the system. This minimizes intervention and streamlines control.

Recovery Objectives

Recovery Time Objectives (RTO) can be stated as the length of time it takes to recover data from a loss event and return it back to service. Tape solutions provide portability and mobility, but they do not fully address a company's RTO. Disk solutions help reduce the recovery time but add cost. Look for a solution that promotes "Disk to Disk to Tape" (D2D2T), bringing the best of both solutions to your environment. D2D2T will help you achieve good RTO and a cost-effective offsite Disaster Recovery plan.

Recovery Point Objectives (RPO) can be stated as the amount of time between backup events. This can also equate to the amount of data at risk of being lost between those backup events. Replication solutions are ideal for business continuity however, they are vulnerable to corruption. Most mirroring

solutions provide multiple copies — either good copies or corrupt copies. For example, most events that lead to data corruption are not immediately identified. Weeks can pass before the virus or other corruption has been detected. A better solution for backup and recovery captures “Points in Time” to protect against accidental deletion, corruption or virus. Be aware that some backup and replication technologies require unacceptable manual processing to re-build the protected data. Conveniences like “User Initiated Restore” help to reduce the administrative burden normally associated with the data recovery.

Open Files

Open files expose a vulnerability of some backup and recovery solutions. Open files are not just files in motion they are also system files, user and system configuration files. Some solutions require expensive third party software to completely back up the open files on a computer. Look for a solution that provides open file backup as a standard feature not an additional cost.

Verification

A system that does not provide validation of the “backup event” is incomplete. Products that state a failure without tracking the progress of the backup will waste time and money. Look for products that “proactively” reinitiate a failed backup. The backup should start from the point of failure and not restart the whole job. It should only include the files that have changed along with those that failed during the original session. It is also important to understand how the files are validated before, during, and after the backup process. No one can recover data that does not exist so be sure to purchase a solution that provides verification of the data and the operation.

Disaster Recovery (Bare Metal Recovery)

Look for a solution that provides true disaster recovery at no additional cost and ensures that you can create the recovery image even if the computer has died. “Bare Metal” Disaster Recovery is one option. Bare Metal recovery allows you to build a bootable CD with an ISO image of all necessary files, including low-level drivers to rebuild any protected system. You can recover the entire system in less time than it takes to normally reload, reconfigure, patch, and update the operating system, significantly reducing your recovery time.

Mail and Database Servers

If you are running a Microsoft Exchange Server, you need to ensure your selection is fully integrated with the Microsoft Application Programming Interface (API) for Exchange Server. It must offer full, log/incremental and differential backups of the server. For maximum flexibility, the solution should also allow for the backup and recovery of individual mailboxes and messages as well as an automated procedure for point in time restores. If you are using SQL Server for your database, take steps to ensure full implementation of the Microsoft SQL API for backup and restore. The system should perform full, differential, log and no-log truncate backups.

Best Practice Data Protection

These are just a few key factors to consider when implementing a business protection strategy. All businesses are vulnerable and only through an effective data protection plan can you minimize impact on the business, if and when a loss should occur. Education and advance planning are key to finding the optimal solution. By taking into account these key factors, you can begin understanding the options available when selecting the best strategy for your business.

Breece Hill assists companies by offering data management capabilities previously available only to large companies and enterprises. Breece Hill has focused on the SMB market for over a decade and helps customers implement an effective business protection strategy by providing backup and recovery solutions that are the easiest to own, operate and manage.

Breece Hill’s BizGuardian™ is the only fully-integrated backup and recovery system being offered today. The BizGuardian backup and recovery appliance combines disk and tape along with the operating system and applications with data protection policies that represent “best practices” out of the box. With the BizGuardian, companies receive rapid data protection, quick access to restore lost files and effortless off-site disaster recovery. For more information about Breece Hill, visit www.breecehill.com.



Breece Hill, LLC
246 S. Taylor Avenue
Louisville, CO 80027
www.breecehill.com

Tel 303.664.8200
Toll free 800.941.0550
Fax 303.664.8299
Europe Tel +44.870.165.5500