WHITE PAPER

Can Your Business Survive Application Downtime?

Affordable solutions for small and medium companies to mitigate risk and prevent losses

Sponsored by

DECEMBER 2009

mclellan creative RESEARCH

Executive Summary

Large businesses understand that effective, robust business continuity (BC) and disaster recovery (DR) solutions are critical to sustaining the health and well-being of the organization when unpredictable downtime or disaster strikes. They rely on enterprise-class, best-of-breed solutions to help them manage and mitigate risks so they can operate 24x7 under ideal conditions or in the aftermath of any type of catastrophe.

Unfortunately, small and mid-size businesses mistakenly believe that these types of products and services are not affordable or available to them. Consequently, they often limit their investment in necessary disaster protection tools and make compromises regarding which type of assets get the most protection. Many rely on very basic data recovery solutions that are often paired with legacy or manual methods to back up and protect data and other business assets. This is a flawed strategy that puts their continued existence at high risk. Small and mid-size companies do not realize their largest financial losses can result from common everyday events. The greatest potential for business failures occur, not as a result of natural disasters, but as a consequence of human error or application and hardware failure. And following a major data loss, without a DR plan and solution, the majority of them may be out of business within a year.

This paper details the ways in which all businesses are at risk and explains why small to medium-size businesses are particularly vulnerable. It also provides solutions designed for small and mid-size businesses. The key points explained within this paper include the following:

- Shortcomings of common backup and recovery methods.
- Reasons why common backup methods can't provide sufficient protection or easy restoration of applications and data following a catastrophe.
- Most useful features and benefits of today's leading backup and recovery solutions.
- Suggestions for how small and mid-size businesses can achieve cost effective, affordable, and reliable disaster recovery and business continuity solutions.
- How managed services can provide small to medium businesses with similar solutions to those used by large corporations.

Finally, the paper describes the actual experiences of a mid-size company. It details how the products they chose to protect their business assets were able to increase their productivity and improve key business processes. It also illustrates how their decision ensured that the business never missed a beat when Hurricane Wilma struck South Florida.

The greatest potential for business failures occur, not as a result of natural disasters, but as a consequence of human error or application and hardware failure.

Natural, accidental, or man-made disasters are often more devastating to small and medium-size businesses than to large organizations.

Any Type of Downtime Can Harm Business

Whatever its size, no organization is immune from the many types of unforeseen or unpredictable causes of data loss and damage as well as server and application downtime including:

- Human error (end-user and IT administrator)
- Crucial hardware failure (server, network and storage)
- Virus, worm, deliberate sabotage, or malware attack
- Water damage from a burst water main, frozen pipe, etc.
- Planned or unplanned power outage due to a local construction project
- Catastrophic natural events such as a hurricane, tornado, flood, mudslide, earthquake, fire, etc.

Unplanned downtime impacts a company's productivity, revenue, customer confidence, and company reputation. The business is also impacted when there is any loss of critical data such as:

- Customer database
- Customer, business, and data transactions
- Stored financial data and current financial transactions
- Legal data and transactions
- Company Internet or Intranet
- Valuable and historic data including email communication with partners, vendors, and customers

At the very least, loss of critical data, applications, or systems can seriously impact a company's ability to transact business immediately following a system outage, catastrophic or not. It can take hours, days, or even months to restore applications and servers after such an event. In addition, there may be increased costs associated with recovery such as unplanned hardware, software or infrastructure purchases. There may be other expenses associated with restoring the business back to full operation including renting temporary office space, building repair costs not covered by insurance, and additional staff.

Natural, accidental, or man-made disasters are often more devastating to small and medium-size businesses than to large organizations. Small and mid-size businesses don't have the IT budget, bandwidth, hardware, or knowledge to assess the risks of calamitous events or to develop or purchase the same type of effective, comprehensive recovery and continuity plans of large enterprises. Furthermore, the US Small Business Administration (SBA) advises companies to "develop a schedule for backing up all computer records and keep current copies of all paper and computer files off-site and accessible."[1] Without these precautions it may not be possible to recover everything

1 http://www.sba.gov/idc/groups/public/documents/sba_homepage/serv_disprep_planningguide.pdf

that is lost if the servers or building housing this type of data are destroyed by a catastrophic event.

Although the largest financial losses and business failures happen as a consequence of natural disasters (e.g. earthquakes, floods, etc.), that is not the primary cause of data loss. This is best illustrated in the 2007 report, *Impact on U.S. Small Business of Natural & Man-Made Disasters.* In this report, SCORE and HP republished the following statistics from the University of North Carolina's Information Technology Service about common ways that businesses experience data loss: [2]

- A hard drive crashes every 15 seconds.
- 2,000 laptops are stolen or lost every day.
- 32 percent of data loss is caused by human error.
- 25 percent of lost data is due to the failure of a portable drive.
- 44 percent of data loss caused by mechanical failures.
- 1 in 5 computers suffer a fatal hard drive crash during their lifetime.
- 40 percent of SMBs don't back up their data at all.

These statistics are particularly poignant because the odds of not being able to stay in business increase substantially whenever a company is unable to recover its data. One of the findings from the 2004 report on Contingency Planning conducted by Strategic Research Corp and DTI/Price Waterhouse Coopers states that "70 percent of small firms that experience a major data loss go out of business within a year." [3]

"70 percent of small firms that experience a major data loss go out of business within a year."
—Strategic Research Corp and DTI/Price Waterhouse Coopers

Even though disasters occur with inevitable and incessant regularity in the US and throughout the world, far too many small businesses fail to take adequate precautions to protect their applications and data. A Harris Interactive survey of 597 computer users reported the following:

- 85 percent of the respondents say they are very concerned about losing important digital data.
- Only 25 percent of those respondents who indicated they are concerned say they frequently back up files.
- 37 percent of the survey's respondents admitted to backing up their files less than once a month.
- 9 percent admit they never backed up their files.
- More than 2 percent said backing up information is on their to-do list, but they seldom do it.[4]

Traditional and Legacy Backup Solutions Alone are not good Enough

Protecting business data and essential applications is contingent upon finding the most effective products and processes that will allow small and mid-size businesses to

2 http://www.score.org/pdf/HP_Download_ImpactofDisaster.pdf

3 Contingency Planning, Strategic Research Corp and DTI/Price Waterhouse Coopers (2004)

4 Harris Interactive survey done for the Imation Corp., Reality Times, September 2002.

"An estimated 25 percent of businesses do not reopen following a major disaster."
—Institute for Business and Home Safety

continue operations in the event of data loss. On its Disaster Preparedness web page, the US Small Business Association writes the following:

"For small business owners, being prepared can mean staying in business following a disaster. An estimated 25 percent of businesses do not reopen following a major disaster, according to the Institute for Business and Home Safety." [5]

Disaster recovery and business continuity solutions for small and mid-size businesses must be flexible enough to optimize their limited resources while minimizing both planned and unplanned downtime. Equally important, and to be attractive to companies with small budgets and limited resources, the solutions must be capable of balancing cost and risk while maintaining the availability of critical systems, applications, and data.

The most common techniques used are traditional backups to tape or disks, RAID arrays, and clustering. While each of these provides limited value in certain situations, none of them should be used as the exclusive solution for disaster recovery and business continuity protection.

Traditional Backups

Most small and many mid-size organizations rely on traditional backups, such as tape drives or CD-ROM, as their only means of making copies of data and applications. While this method does provide a basic data recovery solution, it does have its challenges. For example, if the backup tapes or disks are stored within the same location as the primary servers or even locally in the same city, they are vulnerable to localized disasters like fire or flood, along with the servers and data you are protecting. Tape drives are notorious for failures and tape can break or be easily damaged by poor handling or atmospheric conditions (heat, humidity, etc.).

Many routine events, including server migration, maintenance, and application and system testing of operational servers can disrupt business operations. Probably one of the biggest challenges with traditional backup and restore is how long it takes to restore data after loss or damage, especially if the data is on tape and stored at a remote location for DR purposes.

Even the US Small Business Administration recognizes that tape backup alone is not sufficient for its own needs. The following is an excerpt from a case study sponsored by Iron Mountain that illustrates the problem the organization faced.

"Data backup and recovery had long been the most challenging component of the SBA's disaster recovery plan, requiring daily attention and coordination across each of

5 http://www.sba.gov/services/disasterassistance/disaterpreparedness/index.html

its locations. The agency had been relying on tape-based backup systems. However, it was virtually impossible for the SBA's IT department to ensure that every location was consistently backing up its data properly and vaulting it off site on a regular basis. As a result, there was significant risk of operational disruption due to the possibility of an office losing critical data due to a human error, system failure, server crash or broader disaster. The SBA recently eliminated this vulnerability in its disaster recovery plan by adopting Electronic Vaulting to automate data backup and recovery across multiple locations." [6]

Redundant Array of Independent Disks (RAID)

Some organizations rely on a redundant array of independent disks (RAID) as a cost-effective disaster recovery solution. RAID achieves a high level of storage reliability by dividing and replicating data among multiple hard disk drives to increase data reliability and performance. When these multiple disks are set up in an array, they are viewed by the operating system as one single disk. RAID differs from traditional backup, because it is often used to mirror systems and thereby create an up-to-date copy of the data. This copy can then be used for recovering data in the event of any type of disaster.

Although RAID appears to be a sensible and relatively economical data recovery solution, RAID systems generally require someone with the necessary skills to manage and keep them properly configured. RAID solutions work fine in many situations, but unless the RAID is kept at a remote site, it is not safe from such natural disasters as hurricanes or floods. RAID is also not the most ideal solution because it does not protect data from human error, virus or malware attacks, or other similar failures.

One of the problems of using RAID for disaster recovery is discussed in an article in the Disaster Recovery Journal, *SATA RAID: Enterprise-Class Data Protection and Recovery for Everyone*. The author writes, "RAID complements rather than replaces any backup procedures that an organization may already have in place. For example, a hidden, local array is protected from software or user threats, but not from fires or floods. Thus, a remote backup procedure is still required for business-critical data."[7]

Server Clusters

Many organizations have alternatively turned to server clusters as a way to provide higher availability, reliability and, more importantly, business continuity. A server cluster is a group of servers that are linked together so that for all practical purposes they appear and function as a single server. The servers in each cluster are designed to work together to protect data. They also keep applications, processes, and services running in the event of any of type of hardware, software, or data failure.

"RAID complements rather than replaces any backup procedures that an organization may already have in place."
—Disaster Recovery Journal

6 http://www.ironmountain.com/resources/serverprotect/smallbusiness.pdf

7 Steve McIntosh, *Disaster Recovery Journal,* Winter 2005, Vol. 1: "8ATA RAID: Enterprise-Class Data Protection and Recovery for Everyone". *http://www.drj.com/articles/win05/1801-17.html*

The challenge of using clustered servers for business continuity is that they are too costly and complicated for many midsize and most small businesses. In addition, local clustering cannot protect servers and their applications if disaster strikes at the principal site of the server cluster.

Whether companies rely on any of these backup technologies or worse, use a less reliable method like non-commercial backup software (or free-ware), the challenges are still the same. A backup is only good if it was done correctly and in a timely manner. And it is only useful if the data is good and can actually be read from the backup media. Under ideal situations these backup strategies can protect a business, as long as the backup media and the operator perform as expected. Apart from lacking the efficiency and automation of more recently introduced disaster recovery and business continuity products, traditional backup and restore recovery time is typically too long for most critical applications and data. In addition, periodic backups do not support the recovery point objectives needed—especially if backup is only performed once a day or less, and it does not address server or application outages.

Helping Organizations Weather the Storm of Unpredictable Catastrophes

The modern business ecosystem—no matter what the size of the organization—is a complex mélange of stored data originating from and being sent to multiple destination sources and stored on a variety of storage devices such as DAS, NAS and SAN. In the normal everyday work environment, this data is under siege from a variety of events including increasingly sophisticated cyber attacks, errors made by end-users or administrators, application errors, and even malicious attacks by disgruntled employees. It is now possible for small and mid-size businesses to leverage this type of comprehensive business continuity and data recovery technologies previously only available to large corporations. And they have a choice of robust, proven packaged solutions, turnkey, managed services, or a combination of both. Here is an overview of some of these options.

It is now possible for small and mid-size businesses to leverage this type of comprehensive business continuity and data recovery technologies previously only available to large corporations.

Real-Time Replication

Host-based, data replication software solutions provide organizations with real-time, continuous data protection for file servers, as well as database applications and production email servers. These products rely on failover (aka replica) servers that are typically housed at a remote location to cover both business continuity and disaster recovery needs. Replication software first synchronizes your production servers and failover servers over the LAN or WAN and afterwards, only the “changes” to your database records, files and data are replicated, helping minimize bandwidth requirements. The remote location can be a data center or a remote office belonging to the company or a third-party service provider.

These products deliver real-time, high availability business continuity and disaster recovery protection and support for multiple platforms.

More comprehensive versions of this type of software incorporate real-time health monitoring of servers and applications. This allows automatic or manual failover to your replica servers. As soon as the system detects an application or server problem, the system notifies the IT administrator and automatically fails over and redirects users to the replica server. The system also supports manual failover control to eliminate system downtime during server or application testing or maintenance, or to migrate to a new server or migrate from a physical to a virtual server.

Usually systems with this level of sophistication provide built-in automated disaster recovery testing to permit IT administrators to schedule periodic, non-disruptive testing of the failover server and application. This type of testing ensures the system will perform as required in the event of any type of outage or disaster without any impact on user or IT productivity.

Continuous Data Protection

Continuous data protection (CDP) should be a part of any organization's data protection technologies. It simplifies the recovery of data in most types of storage and server environments. In the aftermath of an accidental data loss or human or malicious corruption of data, the availability of a CDP solution with data rewind capabilities enables IT to roll the data back to a point in time where they know the data is good.

Continuous data protection is complementary to traditional backup solutions because it provides continuous protection versus periodic protection.

Continuous data protection is complementary to traditional backup solutions because it provides continuous protection versus periodic protection. Preferably, this solution is integrated with the replication solution, as replication solutions will most likely replicate the deliberate or accidental changes to the data on the failover server before anyone can detect that a problem occurred. When that happens, without an integrated CDP solution, it is difficult and sometimes impossible to go back to the precise point in time where the data is still good. This usually means that IT has to pull the disks or tape containing the last known backup to restore the integrity of the data on the primary server, which often results in a gap where data is missing or lost entirely. Another benefit of replication with integrated CDP is that the process of data rewind may be performed on the replica server instead of the production server, eliminating a disruption in service.

Automated Disaster Recovery Testing

Automated disaster recovery testing is an essential part of any disaster recovery solution portfolio because it allows IT teams to schedule periodic, testing of the fail-over server without disrupting the production environment or continuing replication protection or impacting IT productivity, employees or live assets. It ensures that the applications and

data residing on the failover system are completely ready to take over with no disruption to a production environment should any type of catastrophe or human error happen.

Hosting and Managed Services for Business Continuity and Disaster Recovery

For small and medium-size businesses that don't have a remote location to use, or don't have the capital budget or IT staff or experience to consider the aforementioned technologies, there are a range of affordable and easy alternatives: hosting and managed business continuity and disaster recovery services from a variety of vendors. Hosting service providers offer the facilities, floor space, equipment and staff for SMBs without their own remote locations. All types and sizes of organizations have opted to use a turnkey managed services offering because there is no hardware or software to purchase, install, manage or maintain and no ongoing need to involve their internal IT staff in supporting and running the software and systems.

All types and sizes of organizations have opted to use a turnkey managed services offering because there is no hardware or software to purchase, install, manage or maintain and no ongoing need to involve their internal IT staff in supporting and running the software and systems.

Managed disaster recovery and business continuity services incorporate an enterprise-class level of protection without requiring an organization to purchase, set up, manage, test, and run the hardware, software, and required facilities and infrastructure. This means there are no upfront costs, which is especially important for small and medium-size businesses that mistakenly believed this level of disaster recovery protection is out of their reach financially. This type of service is typically offered on an annual subscription basis with affordable monthly service fees. There are also no management or maintenance headaches because the service provider is hosting the service at its own remote site. Since there is no equipment to buy and install, managed services can typically be deployed in a day or two.

The Proof is in the Success of Others

Nothing illustrates the importance and value of having a sound disaster recovery and business continuity solution better than the experiences of actual customers who have installed and had to rely on this type of technology when disaster struck their business. Here is an example of one such company that is grateful it had the right type of systems in place when disaster struck.

A large law firm in Florida with offices in 2 cities provides corporate practice and litigation as well as a wide range of legal services and business solutions for its domestic and international clients. The firm employs 500 people, supports 600 email boxes, and has at least 4.5 million legal documents that have to be protected. When Hurricane Charley hit the region in 2004, the city turned off the power grid, effectively shutting down the half of the firm that was located in the direct path of the storm.

Since the law firm practices in one of the most volatile weather regions in the United States, the firm's IT officials recognized the need for a reliable disaster recovery plan as well as a product that not only replicated the data but also had failover capability. The firm also saw the opportunity to use the solutions it acquired to consolidate infrastructure and improve WAN communications across its networked locations.

The law firm implemented a recovery management solution that included continuous data protection using a secondary data center in Chicago, which now serves as the firm's failover site. By deploying this technology the law firm was also finally able to test the data on its replica server.

Most significantly the recovery management solution that the firm implemented was able to provide 100 percent data and system availability during one of Florida's worst recent storms—Hurricane Wilma. Just before the storm hit Florida, the firm made the decision to manually failover its operations over to the replica data center in Chicago, to eliminate any potential system downtime. According to officials it took less than 15 minutes to bring the Chicago failover center online, and their business never stopped running.

Conclusion

When disaster strikes, whether simple data loss or complete site loss, organizations can be certain it won't be at a time that is convenient. It won't take into consideration whether or not the business can afford the downtime or the accompanying losses to data, applications and the viability of the business itself.

Increasingly more small and mid-sized companies are running 24x7 operations and using more mission critical applications than at any other time in history. Relying on legacy or traditional data backup solutions is just not sufficient because any type of downtime adversely affects a company's productivity, revenue, and reputation.

What solutions it employs and how an organization guards against everything man or nature has to throw at it will ultimately determine its fate. The US Small Business Association agrees and gives the following advice to business owners on its disaster preparedness webpage:

"Getting back to business after a disaster depends on preparedness planning done today. Small business owners invest a tremendous amount of time, money and resources to make their ventures successful, and yet, while the importance of emergency planning may seem self-evident, it may get put on the back-burner in the face of more immediate concerns." [8]

"Getting back to business after a disaster depends on preparedness planning done today."
–Small Business Administration

8 http://www.sba.gov/services/disasterassistance/disasterpreparedness/index.html

Just like enterprises, small and medium businesses need to have a combination of disaster protection technologies and business continuity solutions already in place—above and beyond a well documented plan of action. An investment in best-of-breed, enterprise class, hardware, software, and/or managed service solutions is essential if an organization expects to protect its most vulnerable and precious assets.

Today affordable, comprehensive, integrated high availability, disaster recovery and business continuity solutions are available as either products or managed services. With these solutions, no organization—large, medium, or small—has to worry about losing its data, applications, and ability to recover and continue operating its business when any type of disastrous event occurs.

For more information about CA XOsoft products, please visit http://arcserve.com

About McLellan Creative Research

McLellan Creative Research (MCR) is a leading research company providing market intelligence and insights for the information technology, healthcare and consumer technology markets. MCR helps IT professionals and business executives understand emerging technology trends and solutions, develop creative strategies and make decisions on technology purchases. In addition to research and writing services, MCR also offers worldwide translation and localization services through its partners.

Founded in 1995, MCR creates research documents for companies ranging from global enterprises to small startups. The company's expertise includes the development of individual research documents, white papers and thought leadership. A division of McLellan Creative, MCR is headquartered in Ashland, Oregon and its team of technology research associates is located throughout the U.S. and in Europe.

For more information about McLellan Creative Research, visit www.mclellancreative.com.