SIX DATA PROTECTION TIPS FOR SMBs

Whitepaper
Double-Take Software, Inc.
Published: August 2009

Just like major corporations, small and midsize businesses (SMBs) are increasingly reliant on the critical data stored on their servers. Limited resources and vulnerability to interruptions put small and midsize businesses at higher risk, and relying on native backup for a small business server can leave gaps in the disaster recovery plan. While native backup for Windows Small Business Server provides a small measure of protection, periodic tape backup can leave small businesses vulnerable to data and time loss in quantities they cannot afford. The key to getting back on track quickly is a comprehensive disaster recovery plan, including fast access to an up-to-the-minute copy of your data. This whitepaper provides six tips for an SMB approach to protecting critical data. These tips used in conjunction with Double-Take® Availability from Double-Take® Software can help SMBs defend against crippling downtime and data loss.

Depending on Data

It doesn't matter if you are a billion dollar firm or a twenty-person regional service provider, more likely than not you depend on your data for day-to-day operations. Recent events such as terrorist attacks, rolling blackouts, complex viruses and devastating natural disasters remind us how vulnerable our critical electronic data can be[1] – but studies show small and midsized businesses (SMBs) aren't doing much to protect themselves from data loss. In a recent article, Gartner reported, "SMB management is not typically focused on what might be viewed as 'hypothetical' disaster scenarios."[2]

Not only have the risks changed, the culture of doing business has also changed. New factors that increase the impact of lost data include the exponential growth of critical data generated every day, customer expectations that services resume rapidly after a business disruption and the increasing need to access data almost around the clock.

Today's data protection challenges pose substantial risks to companies of all sizes, but they pose the greatest risk to small and midsize businesses. SMBs often don't have the staff or budget for acceptable disaster recovery and there is often no recovery plan, no recovery site, or the recovery site is not far enough away to protect the primary site in case of a natural disaster. SMBs typically have their critical data all on one server. If the server goes down, most offices have to get that server running and fully restored right away, or face costly consequences. SMBs in regulated industries are also subject to the same data availability and data protection requirements as large corporations for regulations such as HIPAA, FDA Part 11, Sarbanes-Oxley and SEC Rule 17 – but without the budgets necessary to meet the requirements. Finally, cash flow disruptions are often fatal for SMBs. In his article "A Small Business Approach to Computer Downtime", Adian McDermott estimates downtime can cost a small business between $200 and $800 per incident, per PC.[3]

Small Business Server: Is native backup enough?

Microsoft® Windows® Small Business Server (SBS) provides greater flexibility and capacity for small businesses by offering many of the features used by large companies – e-mail, Internet connection, Web sites, remote access, support for mobile devices, file and printer sharing, backup and restore. SBS also provides a native

[1] In his Global Finance article "Is Today's World Becoming Riskier?" International Financer Ajay Garg comments that although his question is technically unanswerable, the nature of risk has changed due to our ever-increasing dependence on technology.

[2] Witty, Roberta J., et al. "SMBs Must Raise Awareness of Importance of Business Continuity/Disaster Recovery." Gartner.com, 5 November 2005.

[3] McDermott, Adian. "A Small Business Approach to Computer Downtime" www.user_groups.net.

utility for performing basic periodic backup. However, relying on native backup to cover all of the bases in an emergency or disaster may leave a business vulnerable to potentially crippling gaps in protection. Tape and disk-based backup can only restore data to the point of the last good backup, which was most likely the night before; any data created since the last good backup will be lost. If the most recent backup was incomplete or corrupted, then you're forced to use the next most recent backup and lose even more data. Backup recovery time can also be below a business's recovery time objectives since the data must be restored from the proprietary backup medium to disk before it can be utilized.

Are you planning to succeed?

While an optimistic outlook is an important ingredient in growing a small business, disaster preparedness is one occasion when it pays to be a pessimist. In a recent article about business continuity, the United States Small Business Association (SBA) called small businesses 'the backbone of the nation's economy'. They report that small businesses alone account for more than 99% of all companies with employees, employ 50% of all private sector workers and provide nearly 45% of the nation's payroll. Yet, small to medium businesses are the most vulnerable in the event of an emergency because most have not taken the necessary steps to prepare. While it's hard to argue with the importance of preparing your business for an emergency, it's easy to put off planning and implementation due to day-to-day concerns and resource constraints. However, the SBA estimates that 25 to 40% of businesses do not reopen after a disaster or long-term business outage. In the wake of recent natural disasters and the current political climate, the SBA is emphasizing to small businesses that getting back to work after a disaster depends on *how well you prepare today*.

Some questions small businesses should ask themselves are:

- Are we prepared to relocate temporarily?
- Do we have copies of, and access to, vital business records? (The SBA recommends backup data is stored at an offsite location at least 50 miles away from the main site.)
- Do we have access to vital business applications? (emergency payroll, accounting, access to suppliers and resources)
- How much data would we lose in a disaster between backups?
- How quickly can we recover from a disaster?
- How long would we be without a connection to our customers?

A Common Risk Scenario

Tuesday 4 p.m. The server crashes at Smith and Johnson law office. Staff can't access e- mail, the client database, appointment calendar, court schedule, research data or project directories. In a best-case scenario, by Tuesday evening the reseller arrives with parts necessary to repair the server and restores the new server from the Monday night tape backup. By Wednesday morning, users can resume work – but all of Tuesday's data and hours of productivity have been lost. A more likely scenario is that the reseller doesn't have all of the parts in stock or they don't have a resource available to install them. They call for replacement parts, but they don't arrive until Wednesday. Wednesday afternoon, the reseller repairs the server and begins the restoration process from the Monday night tape backup. On Thursday morning, users can resume work but the most recent data they can access is from Monday night. Over a day of productivity and data are lost. The worst-case scenario is that the reseller doesn't have all of the parts in stock. They call for replacement parts, but they don't arrive until Wednesday. Wednesday afternoon, the reseller repairs the server and tries to restore from the Monday night backup, but the Monday night backup is bad, so they have to restore from Sunday night's backup. By Thursday morning, users can resume access to the server applications, but they can't access data from later than last weekend.

What can a small or midsize business do to minimize the potentially crippling impact of lost data and downtime? The following six tips can help SMBs more effectively protect their critical data and recover faster from downtime.

Six Tips for Protecting Critical Data

Tip One – People, policies and priorities first

Consider having the right people, policies and procedures in place before turning attention to technology strategy. Designate one individual in the company as the data protection owner who is responsible for getting management buy- in, documenting the processes, investigating the options, and directing testing and training.
The data protection owner should form a group to determine what the most critical information to the business is.

This small group should include those individuals whose input will ensure that the most critical business information is protected. In a small business, this may be just the owner or the executive staff. In a midsize business, a manager from each function is probably most appropriate. The data protection owner should identify any relevant regulations that affect the company's data protection priorities. Next, the group should define the critical applications. Given the limited resources in most small and midsize businesses, initially narrow your focus to the one or two core applications where an inability to access key information can quickly start to cost you money, such as your e-commerce site, customer database or e- mail system. By focusing on protecting just one or two critical applications, your data protection goals will be more attainable.

Tip Two – Get the data out of the building
It is extremely important to get your data out of the building and out of harm's way. The ideal offsite location is distant geographically so it remains unaffected by large-scale disasters, such as earthquakes and hurricanes. Consider what the most likely threats are to your place of business.

Is it local power outages? How far away would you need to store the data to be on a different power grid?

Is it earthquakes or hurricanes? Keep the backup data at least an area code away.

Is it most likely to be server failures? Think about what could be done for more rapid recovery of the production machine.

Think creatively about how you can cost-effectively backup the data remotely. For example, if your office is in New York City and your IT administrator lives in New Jersey, you might be able to setup a backup server in their home that is connected to the main server by DSL or cable.

Tip Three – Calculate the costs of downtime
For your peers to appreciate the gravity of the problem, you may need to estimate the downtime costs for employees, suppliers and customers if they can't access critical information. The following method provides a simple way to estimate the average cost per hour of downtime.

Cost Per Occurrence = (To + Td) x (Hr + Lr)

To = Time / Length of Outage

Td = Time Delta to Data Backup (How long since the last backup?)

Hr = Hourly Rate of Personnel (Calculate by monthly expenditure per department divided by the number of work hours.)

Lr = Lost Revenue per Hour (Applies if the department generates profit. A good rule is to look at profitability over three months and dividing by the number of work hours.)

Next, define the recovery objectives for your applications. The best way to quantify your objectives is with a Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each application. The RTO for an application is simply the goal for how quickly you need to have that application's information restored. For example, perhaps 4 hours, 8 hours, or next business day is tolerable for e-mail systems. The RPO for an application is the goal for how much data you can afford to lose since the last backup. Is it 2 minutes worth, 20 minutes or 2 hours? Then estimate the costs to achieve your RTO and RPO for each application.

Finally, get the senior management's understanding and agreement with your downtime cost estimates and required RTO and RPO goals. Once everyone has agreed on the cost of downtime and the company's RTO and RPO goals, it's easier for everyone to agree on the data protection strategy and budget. For example, if you can get the business owner or executive team's agreement that the company's downtime costs are approximately $80,000 per year, they are more likely to agree that $40,000 is an appropriate data protection budget.

Tip Four – Think beyond tape

Once you have established how quickly you need to recover key applications (RTO), how much data you can afford to lose (RPO) and your budget, you can select the appropriate technology solution. Like many SMBs, you are likely to discover that traditional backup technology won't be enough to achieve your RTO and RPO goals for critical applications because of the propensity for failure and the long time to recover your data before you can access it again.

For SMBs whose critical applications run at multiple remote locations, the quality and consistency of on-site tape backup is also an issue. Few companies of any size have technical experts in branch locations who can clean and maintain tapes, ensure that they are properly backing up the site data, and execute a recovery when needed.

Small and midsize businesses face a conundrum: tape backup systems are inexpensive and fairly reliable, but they offer poor RPO and RTO for critical applications, and they are usually ineffective for remote locations. Hardware mirroring technology, which uses remote copy technology to provide synchronous mirroring between two sites, offers excellent RPO but it is prohibitively expensive for a small or midsize business to buy and manage. Plus, it is less than ideal for backing up remote locations which often have low-bandwidth connections and hardware mirroring requires large dedicated bandwidth between sites.

Solutions based on asynchronous software-based replication can achieve the acceptable RPO for critical applications without the cost and complexity of the synchronous replication approach. With software-based replication, only the bytes that change are replicated. When compared with synchronous replication solutions, this approach offers lower load on the production servers, faster updates and the ability to send replication updates across low-bandwidth Internet networks. Software-based replication solutions also provide application and server fail-over for excellent RTO, so your users can continue working within minutes of a failure.

Tip Five – Make it easy for users to restore themselves

Most SMBs don't have the IT resources to respond to individual requests to restore files. Fortunately, solutions like Microsoft's Windows Storage Server 2003 make it easy for users to restore files themselves. Windows Storage Server 2003 can be configured to take a snapshot of the data on a server twice a day, for example. Should a user delete or make unwanted permanent changes to a document, they can simply select the file from any snapshot by right clicking on the file, selecting "Properties", viewing all the versions of the file and selecting the one they want.

Tip Six – Make sure you really can restore

It's important to make sure you have thought through how to restore your critical applications quickly – either locally or at a different location. Do you have fast access to all of the components you need to recover? What are the specific steps needed to restore a failed server? What would you do if you had to move the company's operations and employees to another location?

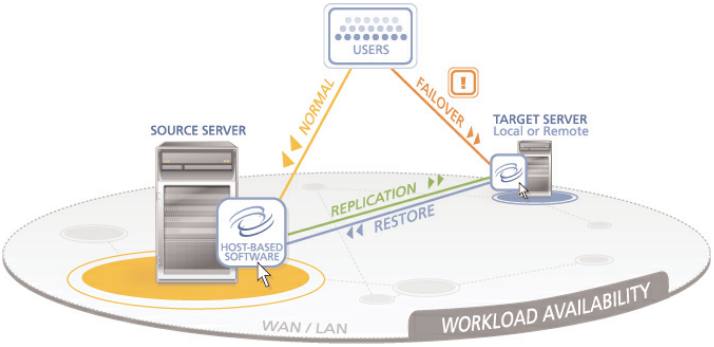
Double-Take Availability can help you recover at another location or recover a branch location quickly, and because it only replicates the data that's changed, it works well over long distances even with low bandwidth connections.

Double-Take® Availability – The Solution for SMBs

Double-Take Availability is the most effective way for small and midsize businesses to experience the data protection benefits of asynchronous software replication.

Today, Double-Take Availability is the most relied-upon solution for real-time replication of critical data and automated failover for application availability. Double-Take Availability is Microsoft® Windows® 2000 and 2003 certified at all levels, one of the few replication products to have achieved this level of certification. It delivers protection that is better or comparable to many hardware based solutions, but costs tens of thousands less.

Double-Take Availability replicates changes to files at the byte-level from any Windows Server to any other Windows Server across any IP-based network. It installs on each server and monitors the real-time changes that are occurring to files and it replicates those changes to another server and applies them to a secondary replica of the data. All changes are sent and applied in the exact logical order that they occurred on the production system, guaranteeing a crash-consistent copy of data on the secondary system.



Beyond minimal protection

Double-Take Availability goes beyond the minimal protection of periodic backup by providing disk-based continuous data replication, ensuring minimal data loss, and enabling fast recovery from any disaster or outage – priced with the small business in mind.

Double-Take Availability continuously captures byte-level changes as they happen and replicates those changes, locally or to a recovery site miles away. Because changes are captured in near-real time, in the event of a disk crash, power failure, human error or natural disaster, you may only lose seconds of data – instead of hours or entire days. Unlike other costly solutions that limit your geographic options or require special network connections, Double-Take Availability works over any distance using your existing IP networks even the Internet. You can station your target server as far away as you would like to ensure maximum protection against disasters.

Because Double-Take Availability replicates only the bytes that change, it uses the minimum bandwidth required to backup your data. Features like Flexible Bandwidth Scheduling and Intelligent Compression allow you to control when replication occurs and how much bandwidth Double-Take Availability is allowed to use.

When disaster strikes, you can use the secondary disk-based copy of your data to restore the production server within moments. Double-Take Availability is server, storage, network and application independent and works with the services you have today.

Full-Server Failover: Protect more than just your data

But there's more to protecting your systems than just protecting the data. The Full-sever Failover feature ensures everything is protected – including the operating system(OS), applications and data. The Full-server Failover feature combines cutting-edge system state protection and recovery capabilities with the real-time replication of Double-Take Availability, ensuring applications are available when they're needed without introducing paralyzing levels of complexity for the small business owner. A single click of a button is all that it takes to completely recover your systems. Because the Full-server Failover feature is protecting the system state of the production server, there's no need to separately manage service packs, application updates or hotfixes on the standby server, further reducing the complexity of maintaining application uptime.

An Alternate Recovery Scenario with Double-Take Availability

Now, with Double-Take Availability installed on both their critical server and on an inexpensive backup server located in the office manager's home, the Smith and Johnson law office has a better experience than even the best-case scenario described above.

Tuesday 4PM. The server crashes at Smith and Johnson law office. Staff can't access e- mail, the client database, appointment calendar, court schedule, research data or project directories. Within 15 minutes, Double-Take Availability has automatically switched to the backup server, which has all of the data up to Tuesday at 4PM, the very moment of the production server crash. Users can access all of their applications. On Tuesday evening, the reseller or integrator arrives with parts necessary to repair the original production server and begins resynchronizing the production server from the backup server – while the users can still access their data and with all of Tuesday's data intact and with no impact to the business.[4]

[4] Even in the worst-case scenario where the reseller has to order parts, users can continue to work on the target server until the primary server is restored.

Summary

Like major corporations, small and midsize businesses are increasingly reliant on the critical data stored on their servers. However, limited resources and vulnerability to interruptions put small and midsize businesses at higher risk. In the past, small and midsize businesses had could only try to cope with this greater level of risk, but no longer. Plus, relying on native backup for your small business server can put your hard-earned success at risk, and statistics show that a large percentage of small businesses who endure a disaster are not able to reopen. While native backup for Small Business Server provides a small measure of protection, periodic tape backup can leave you vulnerable to massive amounts of lost data and time in a disastrous event. The key to getting back on track quickly is a comprehensive disaster recovery plan, including fast access to an up-to-the-minute copy of your data. Double-Take Availability provides a complete protection and recovery solution at a favorable price for small businesses.