HP OpenView Storage Mirroring white paper

Six tips small and midsize businesses can use to protect their critical data

Data protection challenges—When data is your business 2

Small and midsize business data protection pain points 2
- Tip one: Think people, policies, and procedures first 3
- Tip two: Get the data out of the building 4
- Tip three: Calculate the cost of downtime 4
- Tip four: Think beyond tape to achieve your recovery objectives 5
  - Asynchronous software replication—a better solution for small and midsize businesses 5
- Tip five: Make it easy for users to restore themselves 6
- Tip six: Be sure you really can restore in different situations 6

Conclusion 7

For more information 8

Data protection challenges—When data is your business

Whether you are a billion-dollar financial services firm or a 20-person regional service provider, you are probably increasingly dependent on your data for your day-to-day operations. But the deluge of major virus attacks, multi-city power outages, and natural disasters, combined with the less publicized problems such as equipment failures, network interruptions, or simple human error, all add up to major risks in protecting your business's critical information.

New factors that have increased data protection risks include:

- The exponential growth of business information generated every day means even more and more data must be backed up.
- Customers expect services to resume rapidly after a business disruption—regardless of the circumstances.
- The increasing need to access data almost around the clock has dramatically reduced the time permitted to back up data.

Today's data protection challenges pose substantial risks to companies of all sizes, but they pose the greatest risk to small and midsize businesses.

Small and midsize business data protection pain points

- Limited IT resources for backup and recovery—Many small and midsize businesses have little or no dedicated IT personnel to respond quickly to business interruptions.
- All critical data on one server—If that server goes down, most offices have to get that server running and fully restored immediately, or face costly consequences.
- Regulatory pressures—Small and midsize businesses are subject to the same data availability and data protection requirements as large corporations for regulations such as HIPAA, Sarbanes-Oxley, and SEC Rule 17—but without the big budgets to meet these requirements.
- Cash flow disruptions even more damaging—Business disruptions that cannot be quickly recovered from can quickly start to impact cash flow—something few small and midsize businesses can afford.

Following is a common scenario that highlights the risks to a thriving midsize business.

Tuesday, 4:00 PM: The server crashes, and there is no standby server. Users cannot access email, the customer database, or their project directories.

Best-Case Scenario

Tuesday evening: Their reseller or integrator arrives with parts necessary to repair the server and restores the new server from the Monday night tape backup.

Wednesday morning: Users can resume work, but all of Tuesday's data has been lost.

Lost productivity: A few hours

Lost data: One day's worth

More Likely Scenario

Wednesday afternoon: Their reseller did not have all the parts in stock. They call for replacement parts, but they did not arrive until Wednesday. Wednesday afternoon, the reseller repairs the server and tries to restore from the Monday night tape backup.

Thursday morning: Users can resume work, but the most recent data they can access is from Monday night.

Lost productivity: More than a day

Lost data: Two day's work

Worst-Case Scenario

Wednesday afternoon: Their reseller did not have all the parts in stock. They call for replacement parts, but they did not arrive until Wednesday. Wednesday afternoon, the reseller repairs the server and tries to restore from the Monday night tape backup. However, the Monday night tape is bad, so they have to restore from Sunday night's tape.

Thursday morning: Users can resume work, but they cannot access data from later than last weekend.

Lost productivity: More than a day

Lost data: Everything since last weekend

If the last scenario occurred during the last week of a quarter, it could significantly impact the company's revenue. According to Gartner, "50% of all small and midsize businesses will go out of business within three years if they can't get back their data in 24 hours."

What can small or midsize businesses do to minimize this huge risk to their business? Following are six tips these businesses can use to more effectively protect their critical data and recover faster from downtime.

Tip one: Think people, policies, and procedures first

Before worrying about the technology, you first must have the right people, policies, and procedures in place. One individual in your company should be designated as the "data protection owner." This person should be responsible for getting management buy-in, documenting the processes, investigating the options, and directing the testing and training.

The data protection owner must 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, it is recommended that you initially narrow your focus to one or two core applications where an inability to access key information can quickly start to cost you money. Is it your e-commerce site? Customer database? Email system? Initially focusing on data protection for just your one or two most critical applications makes your most important data protection goals more attainable.

Tip two: Get the data out of the building

It is extremely important that you 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. What are the most likely threats to your business?

- Local power outages—How far away would you need to store the data to be on a different power grid?
- Natural disasters—What steps do you need to take to keep your backup data at least an area code away?
- Server failures—What could be done for more rapid recovery of the production machine?

Think creatively about how you can cost-effectively back up the data remotely. For example, if your office is in New York City and your IT administrator lives in New Jersey, you could set a PC backup server in his or her home that is connected to the main server by DSL or cable.

Tip three: Calculate the cost of downtime

For your peers to appreciate the gravity of the problem, you might need to estimate the downtime costs for employees, suppliers, and customers not being able to access the critical information. The following method provides a simple way for you to conservatively estimate the average cost per hour of downtime for each critical application.

Simple downtime estimate formula
Productivity Impact + Revenue Impact = Downtime Estimate

Productivity Impact: (Average worker rate or salary) x (estimated number of business hours the users would be impacted)

Revenue Impact: (Average monthly gross revenue for the critical application) x (number of business hours the application is impacted)

Next, you should consider defining the recovery objectives for your applications. The best way to quantify your objectives is with Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each application. The RTO for an application is the goal for how quickly you must have that application's information back available after downtime has occurred. For example, for your email system, is it 4 hours, 8 hours, or next business day? 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, 20 minutes, or 2 hours? You then must roughly estimate the costs to achieve your RTO and RPO for each application.

The last and most important part is to get senior management's understanding and agreement with your downtime cost estimates and required RTO and RPO goals. After everyone has agreed on the "costs of downtime" and the company's RTO and RPO goals, then it is easier for everyone to agree on the data protection budget. For example, if you can obtain 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 to achieve your recovery objectives

When 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 now select the appropriate technology solution. Like many small and midsize businesses increasingly dependent on their data, you are likely to discover that traditional tape backup will not be good enough to achieve your RTO and RPO goals for your most critical applications.

For small and midsize businesses whose critical application runs at multiple remote locations (such as retail stores or bank branches), the quality and consistency of on-site tape backup is also an issue. Few companies of any size have the technical experts in branch locations to check that the tapes are properly backed up, maintained, and cleaned, and to execute a recovery.

Small and midsize businesses face a conundrum: Tape backup systems are inexpensive and fairly reliable, but they offer poor RPO ad 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 and RTO, but they are prohibitively expensive for a small or midsize business to buy and manage. In addition, they are less than ideal for backing up remote locations, which often have low-bandwidth connections.

New solutions based on asynchronous software–based replication can achieve the acceptable RTO and RPO objectives for small or midsize businesses' critical applications—without the cost and complexity of the synchronous replication approach. With software-based replication, only the bytes that are actually changed by each write (not the entire block of information or the whole file) 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.

Asynchronous software replication—A better solution for small and midsize businesses

- Provides a near real-time copy of the data on another server without straining your production servers or your network
- Is dramatically less expensive than synchronous replication hardware
- Is much easier to manage
- Works over low bandwidth, so it can effectively back up your remote or branch locations

HP OpenView Storage Mirroring on Microsoft® Windows® Storage Server 2003 is a smart way for small and midsize businesses to gain the data protection benefits of asynchronous software replication.

Windows Storage Server 2003 is a dedicated file and print server that delivers high reliability, availability, and ease of management to small and midsize businesses looking to reduce the complexities and costs of networked storage.

Storage Mirroring software uses asynchronous replication technology—optimized for Windows Storage Server 2003—to deliver continuous data protection and rapid disaster recovery at an affordable price. In addition, the failover capabilities allow businesses to resume rapidly after a disaster or a system outage. In the event of a disaster or system outage, a copy of your data is running on a target server in another location.

In reference to the disaster scenario previously described, the business in this scenario has installed Windows Storage Server 2003 and Storage Mirroring on both their critical servers and on an inexpensive backup server located in the IT administrator's home.

Tuesday, 4:00 PM: The server crashes. Users cannot access email, the customer database, or their project directories.

Tuesday, 4:15 PM: Storage Mirroring has automatically switched to the backup server, which has all of the data up to Tuesday at 4:00 PM. Users can access email, the customer database, and project directories.

Tuesday evening: The reseller or integrator arrives with parts necessary to repair the server and restores the server from the inexpensive backup server—with all of Tuesday's data.

Wednesday morning: Users are back on the primary server; virtually no data has been lost.

Lost productivity: Less than 15 minutes

Lost data: 15 minutes' worth

Tip five: Make it easy for users to restore themselves

If you are like most small and midsize businesses, you probably do not have the IT resources to respond to individual requests to restore files. You cannot afford to have an IT administrator who spends the many hours it usually takes to retrieve and mount a tape and recover individual files. Fortunately, Microsoft Windows Storage Server 2003 makes 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 undesirable changes to a document, they can select the file from any desired snapshot. It is as simple as right-clicking the file, selecting **Properties,** viewing all the versions of the file, and selecting the correct one.

Tip six: Be sure you really can restore in different situations

It is important to be sure you have thought through how you would quickly restore your critical applications—either locally or at a different location. Do you have (or can you quickly get) all the components you would need to recover? What would be the specific steps you would need to take to restore a failed server? What would you do if you had to move the company's operations and people to alternate servers at another location?

Because of the flexible replication approach of Storage Mirroring, two of its greatest strengths are the speed and ease of which it can help you recover at another location or recover a branch location. Because Storage Mirroring only replicates the data that has changed, it works well over long distances, even with low-bandwidth connections.

Conclusion

Like major corporations, small and midsize businesses are increasingly reliant on the critical data stored on their servers. But because of their limited resources and their greater vulnerability to interruptions, small and midsize businesses are even more at risk. In the past, small and midsize businesses often had to live with this greater level of risk. This is no longer true.

By implementing the tips suggested in this white paper, you can significantly reduce your company's downtime risks.

Data protection pain points for small and midsize businesses	How Microsoft and HP software can relieve downtime pain
Limited IT resources for backup and recovery	Windows Storage Server 2003 and Storage Mirroring provide continuous, automatic backup and incredibly easy recovery.
All critical data on one server	With Windows Storage Server 2003 and Storage Mirroring, downed servers can be restored quickly. In addition, the software works on very low-cost servers, making backup servers affordable to companies of all size.
Regulatory pressures	With Windows Storage Server 2003, employees can find individual backup files quickly—without tying up expensive IT resources.
Cash flow disruptions—very damaging	Storage Mirroring on Windows Storage Server 2003 provides failover capabilities to a backup server, so your business can keep running. Major cash flow disruptions do not have to happen just because of business disruptions.

For more information

For more information on how Microsoft Windows Storage Server 2003 and HP OpenView Storage Mirroring can help you affordably reduce your risks from unplanned downtime, visit:

- Microsoft Windows Storage Server 2003: http://www.microsoft.com/storage/
- HP OpenView Storage Mirroring: http://h18006.www1.hp.com/products/storage/software/sm/index.html

5983-1076EN, 02/2005