



# Six Tips Small and Midsize Businesses Can Use to Protect Their Critical Data



2 Hudson Place – suite 700  
Hoboken, NJ 07030

800-674-9495  
[www.nsisoftware.com](http://www.nsisoftware.com)

Powered by  **Double-Take**



## Data Protection Challenges - When Data is Your Business

Whether you're a billion dollar financial services firm or a twenty-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 to 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 has to 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 shrunk the time permitted to backup data.

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

Small and Midsize Businesses Data Protection Pain Points
<p><b>Limited IT resources for backup and recovery.</b> Many small and midsize businesses have little or no dedicated IT personnel to respond quickly to business interruptions.</p> <p><b>Critical data all on one server.</b> If that server goes down, most offices have to get that server running and fully restored ASAP, or face costly consequences</p> <p><b>Regulatory pressures.</b> 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</p> <p><b>Cash flow disruptions even more damaging.</b> Business disruptions that can't be quickly recovered from can quickly start to impact cash flow – something few small and midsize businesses can afford.</p>

Let's look at a common scenario that highlights the risks to a thriving midsize business.

**Tuesday 4PM.** The server crashes. There is no standby server. Users can't access e-mail, 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:** a day's worth.

### More Likely Scenario

**Wednesday Afternoon.** Their reseller didn't have all of the parts in stock. They call for replacement parts, but they didn't 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:** over a day.

**Lost data:** over a day's worth.

### Worst Case Scenario

**Wednesday Afternoon.** Their reseller didn't have all of the parts in stock. They call for replacement parts, but they didn't arrive until Wednesday. Wednesday afternoon, the reseller repairs the server and tries to restore from the Monday night tape backup.

But the Monday night tape is bad, so they have to restore from Sunday night's tape.

**Thursday Morning.** Users can resume work, but they can't access data from later than last weekend.

**Lost productivity:** over 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 a small or midsize business do to minimize this huge risk to their business? Here are six tips every small and midsize business can use to more effectively protect their critical data - and recover faster from downtime.

## Tip One – Think People, Policies and Priorities First

Before worrying about the technology, you first have to 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" should form a group to determine what is the most critical information to the business. 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, we recommend that you 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. Is it your e-commerce site? Your customer database? Your e-mail 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. Consider what the most likely threats are to your place of business.

- Is it local power outages? Then how far away would you need to store the data to be on a different power grid?
- Is it earthquakes or hurricanes? Then, you probably need to keep the backup data at least an area code away.
- Is it most likely to be server failures? Then 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 could simply setup a PC backup server in his or her 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 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
<b>Productivity Impact + Revenue Impact = Downtime Estimate</b>
<b>Productivity Impact:</b> Average worker rate or salary x estimated number of business hours the users would be impacted
<b>Revenue Impact:</b> 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 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 back available after downtime has occurred. For example, for your e-mail 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 worth, 20 minutes or 2 hours? You then need to roughly estimate the costs to achieve your RTO and RPO for each application.

The last and most important part, you need to 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 “Costs of Downtime” and the company’s RTO and RPO goals, then it’s easier for everyone to agree on the data protection 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 To Achieve Your Recovery Objectives

Once you have established how quickly you need to recover key applications (RTO) and 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 business increasingly dependent on their data, you are likely to discover that traditional tape backup won’t 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 who can check that the tapes are properly backing up, maintain and clean tapes, and execute a recovery.

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 use remote copy technology to provide synchronous mirroring between two sites) offer excellent RPO and RTO - but they are prohibitively expensive for a small or midsize business to buy and manage. Plus, 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 business' 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

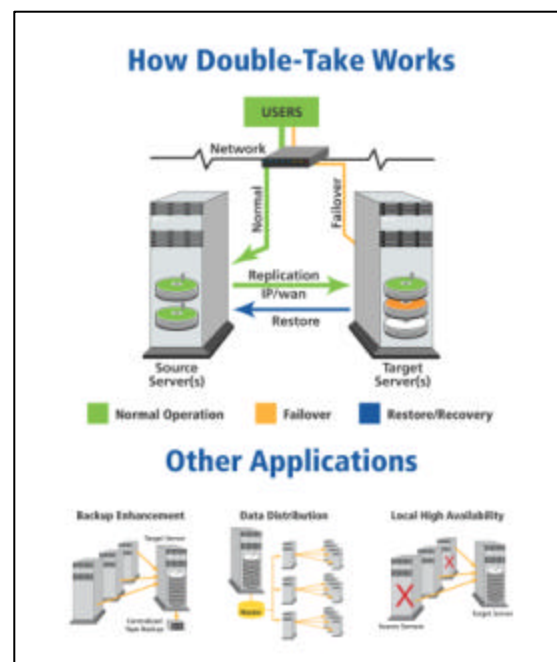
- Provides a near real-time copy of the data on another server without straining your production servers or your network
- Dramatically less expensive than synchronous replication hardware
- Much easier to manage
- Works over low-bandwidth, so it can effectively backup your remote or branch locations

NSI® Software's Double-Take® 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.

Microsoft's 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.

NSI's Double-Take software uses asynchronous replication technology - optimized for Windows Storage Server - to deliver continuous data protection and rapid disaster recovery – at a price that small and midsize businesses can afford.

Plus, Windows Storage Server 2003 and Double-Take's 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.

Let's look at the disaster scenario we described earlier. The business in this scenario has installed Windows Storage Server 2003 and Double-Take on both their critical server and on an inexpensive backup server located in the IT administrator's home.

**Tuesday 4PM.** The server crashes. Users can't access e-mail, the customer database, or their project directories.

**Tuesday 4:15PM.** Double-Take has automatically switched to the backup server, which has all of the data up to Tuesday 4PM. Users can access e-mail, 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 don't have the IT resources to respond to individual requests to restore files. You can't 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's 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 simply select the file from any desired snapshot. It's as simple as 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 In Different Situations

It's important to make 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 of 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 an alternate set of servers at another location?

Because of Double-Take's flexible replication approach, one of its greatest strengths is the speed and ease of which it can help you recover at another location or recover a branch location. Because Double-Take only replicates the data that's 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, and by leveraging new software from companies like Microsoft and NSI software, you can significantly reduce your company's downtime risks.

<b>Small and Midsize Businesses's Data Protection Pain Points</b>	<b>How Microsoft and NSI Software Can Relieve Your Downtime Pain</b>
Limited IT resources for backup and recovery	Windows Storage Server 2003 and Double-Take are designed to provide, continuous, automatic backup and incredibly easy recovery.
All critical data on one server	With Windows Storage Server 2003 and Double-Take, downed servers can be restored in a flash. Plus, the software works on very low-cost servers, making backup servers affordable to companies of all sizes.
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	Double-Take on Windows Storage Server provides failover capabilities to a backup server, so your business can keep running. Major cash flow disruptions don't have to happen just because of business disruptions.

For more information on how Microsoft's Windows Storage Server 2003 and NSI's Double-Take can help you reduce your risks from unplanned downtime - without breaking the bank - go to:

- Microsoft Windows Storage Server 2003 home page: <http://www.microsoft.com/storage/>
- NSI Software's Double-Take home page: <http://www.nsisoftware.com>



© 2004 NSI Software. All rights reserved.

Double-Take®, GeoCluster® and NSI® are registered trademarks of NSI Software, Inc.. Balance™ is a trademark of NSI Software, Inc. All other trademarks are properties of their respective companies.

Microsoft, Windows Powered, Windows, Exchange, and SQL Server, are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Our Vision

*To be the leading provider of data protection & high availability software solutions for 24x7 business operations*

Our Offer to You

*We would like to become your partner in ensuring the continuous operations of your business.*

*Please allow us the opportunity to talk to you about your specific data protection needs and to discuss our products and services that may apply.*

*Your Data is your business, protecting it is ours !!!*

For more information on NSI's products and services, please contact NSI.

NSI Software - Corporate Office

Two Hudson Plaza, Suite 700  
Hoboken, NJ 07030  
800-775-4674 or 201-656-2121  
Fax: 201-656-2727



NSI Software – Inside Sales

8470 Allison Pointe Blvd. Suite 300  
Indianapolis, IN 46250  
800-674-9495  
Fax: 317-598-0187

Or visit us on the web at [WWW.NSISOFTWARE.COM](http://WWW.NSISOFTWARE.COM)