

# Disaster Recovery for Small Businesses

A disaster recovery plan helps you understand what data is critical to your business operations and how to best protect it from unexpected failures.

## Contents

Are You Prepared?	2
What is Disaster Recovery?	2
Risk Analysis	3
Dangers of Data Loss	3
Business-Class Data Protection	4
Best Practices for Small Businesses	5



In the busy day-to-day operations of most small businesses, there is little time for planning for, or even considering the unlikely event of catastrophic technical failure. This is particularly true of small-to-midsize companies that typically have less IT infrastructure in place. A little preparation could literally save your business. According to the Gartner group, 50% of businesses that experience a major disruption ultimately fail. In fact, evidence available at the National Archives & Records Administration shows that 93% of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year of the disaster. Of those companies, 50% filed for bankruptcy immediately.

Iomega offers a comprehensive suite of products to protect your mission-critical business data; using network attached storage to backup and protect your system along with offsite redundancy will protect your business in case of a disaster. This white paper walks you through the simple process of preparing and implementing a disaster recovery plan. A good disaster recovery plan covers the hardware and software required to run critical business applications as well as the data you will need for a smooth transition in the event of a natural disaster or human-caused failure. First, you need to assess your mission-critical business applications and data, and then understand how to protect them.



## Are You Prepared?

- Do you perform backups regularly on every server and employee hard drive in your organization?
- Do you regularly send your data to a safe, off-site archive?
- Do you have a proven media, drive, software, and automation solution?
- Does your current backup and recovery system meet your business uptime needs?
- Do you use backup rotations to provide good versioning?
- Do you know how fast your data is growing?
- Is your backup scalable for this data growth?

## What is Disaster Recovery?

A disaster recovery plan sounds like a complex business document, but it can be as simple as planning ahead to avoid problems and being prepared in the event a problem occurs. This kind of planning will not only help you in the event of a catastrophic failure, like a fire, but also in more mundane situations, like an employee accidentally overwriting a critical file.



## Risk Analysis

The first step in preparing for Disaster Recovery is risk analysis. Each business faces some unique risks – tornados might be more likely in Kansas while the risk of flooding might be more likely in a waterfront community, for example – but all share the same dangers in losing data. Look at each potential risk, and determine its likelihood and potential monetary impact to your business. If the risk is low or there is no financial impact, you can safely ignore it. In many cases, you may find that you already have a plans or processes in place to mitigate risks and ensure business continuity. You need to understand the parameters for your business' worst-case scenario: is it server down-time at a critical juncture or a long-term loss of facilities? What are your most time-sensitive

### Probability: How likely is a risk to occur?

Some risks we can anticipate based upon history. Certain areas, for example, are prone to flooding. You know when floods are most likely to occurs, and can take special precautions at those times.

Even in the best systems, mechanical and electrical parts wear out eventually. Most components have Mean Time Between Failure ratings; when the equipment nears the end of the shortest MTBF-component, look at preventive maintenance.

Ask your self the following questions to complete your risk assessment:

Business Impact: What would happen if the risk occurred?

How much income is lost for 1 hour, 1 day, 1 week, or 1 month?

How much it would cost (overtime, supplemental staffing, and additional equipment) to "catch up" after an outage of 1 hour, day, week, and month?

What damage might happen to the organization's financial status?

Are there any penalties regulating agencies might levy if you are unable to complete a critical process?

An unexpected shutdown will occur to your business at one time or another; it's just a matter of when.

## Dangers of Data Loss

The key causes of data loss are:

- Viruses
- Software and Application Failures
- File Corruption
- Hard Drive crashes
- Laptop loss/theft
- Natural Disasters
- Power Outages

High-capacity external hard drives or a centralized network hard drive is an easy, manageable solution for most small businesses. These drives offer a better ROI than more expensive traditional tape backup systems. A hard drive, either on your desktop or your



network, runs unattended, unlike tape drives that require human activity to remember to manually insert additional tapes. Rather than juggling and tracking a half-dozen or more tapes with complex processes, you simply use two external hard drives. One drive remains onsite connected to either your network backup device or your desktop computer, performing backups. The other is stored securely offsite for disaster recovery. Switch the two hard drives weekly monthly to update the offsite data and to protect your newest data.

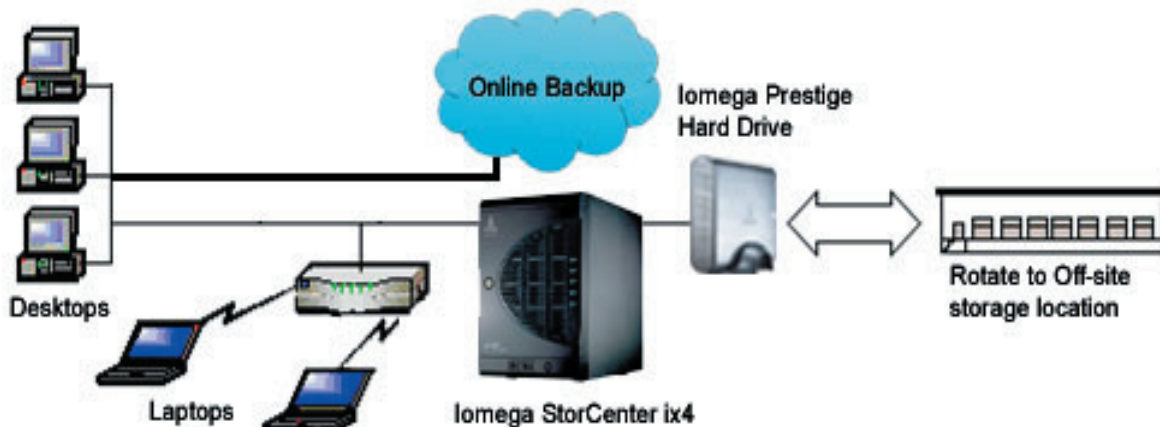
## What Do I Need to Protect?

The specific data and applications you need to back up are unique to your business. Anything you cannot replace easily should be at the top of your list. Based on your risk assessment, you should have a good idea of your critical systems and data. We recommend you back up all data that is difficult or impossible to replace such as email, contact lists, financial records, and office documents. Financial records, such as tax documents and other regulated information is obvious, but it is easier to forget the information we use daily, like your company letterhead or website logos. Most of us store much of our day-to-day work in our email accounts, which are rarely backed up.

## Business-Class Data Protection

For some small businesses, simple backup software that allows automatic copies of key files to a local or network destination will provide solid data protection. Even manually copying key files is better than no backup. For true disaster recovery planning, however, consider the advanced benefits of business-class backup software, like EMC Retrospect:

- Versioning – considering that more than 30% of data loss comes through simple human error (like deleting or writing over a crucial file), maintaining multiple versions of your data is very important. Backups should provide multiple recovery points by saving past versions of files and folders. Avoid merely duplication, which replaces all previous files and retains only the last data backed up. If a problem occurs on a computer and is not caught before the synchronization or mirroring operation is performed, the file would be lost.
- Incremental backups - to save time, backup software should allow you to only backup new and changed files.
- System state – depending on your business needs, you may want to backup device drivers, your system registry, operating system settings, and applications and their settings as well as protecting files and folders.

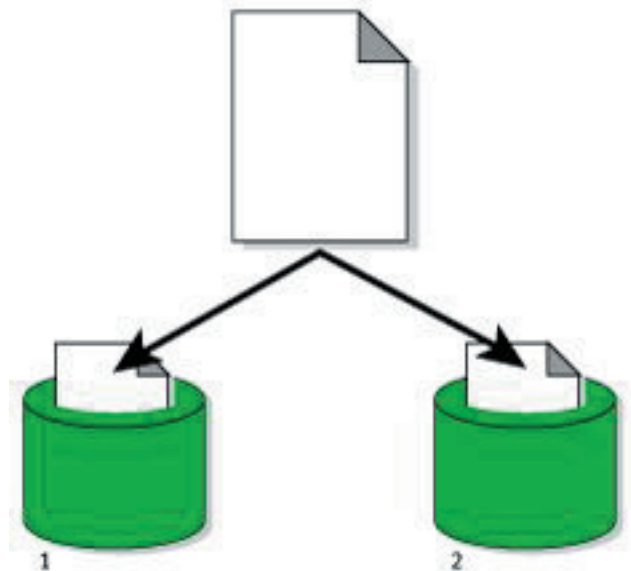


EMC Retrospect also offers an optional Disaster Recovery option, which allows you to create a bootable system image that can be used to replicate or replace your entire system. With this image, you can quickly rebuild critical systems on new hardware.

## Best Practice Backups for Small Businesses

There are simple rules to follow to protect your business in these potential data loss situations.

1. Backup your data on medium that you can trust. Iomega offers a variety of different backup devices to fit any business need. Iomega® REV® Backup drives and removable disks provide a reliable, easy-to-use backup and disaster recovery solution perfect for off-site storage. With EMC Retrospect Software, an Iomega desktop hard drive provides a quick, affordable way to protect against file corruption and human error. For multiple computers in a networked environment, the StorCenter line of network hard drives and NAS devices offer an ideal way to consolidate information for quick replacement. Beware of using CDs to back up critical files, as the medium can degrade over time.
2. Backup all your business data, not just your servers. In 2008, over one-half of all new corporate PCs purchased were laptop computers, and analysts estimate that over 70% of corporate data now resides outside managed servers on laptops. Most organizations rely on mobile users to remember to manually copy business critical information stored their laptops to a network server. Unfortunately, studies show that mobile users rarely follow scheduled backups, leaving sensitive data unprotected and your organization exposed to irreparable data loss. Because laptops are more easily lost or stolen, the risks are even greater, further exposing organizations to considerable legal liabilities and financial risks. Business-class data protection includes continuous backup for laptops as well as servers.
3. Always ensure backup redundancy. If you only have one copy of critical data, regardless of where it is located, you do not have a backup! Keep at least two copies of your mission critical information in a location you can quickly and easily access. If you archive older information, keep multiple copies of your archive. RAID technology provides an easy option for protecting your backups. RAID stands for Redundant Array of Independent Disks, and is a simple way to replicate data among multiple hard disk drives. Iomega's StorCenter NAS devices offer a wide variety of RAID options, combining two or more physical hard disks into a single logical unit. There are three key concepts in RAID: mirroring (copying data to more than one disk), striping (splitting data across more than one disk), and error correction or fault tolerance, where redundant data is stored to allow problems to be detected and possibly fixed. Please note: RAID 0, or striping, does not provide data redundancy. In order to protect your data, you should choose RAID 1 (mirroring) or RAID 5 (available on 4-drive NAS units).
4. Make sure you store another copy of your mission critical data offsite. This can be as simple as storing it on another location, away from your computer. In many risk scenarios, your data is threatened because your site is at risk. Storing your backups in a physically secured offsite location may seem too expensive for small business, but online backup provides an affordable answer.



*RAID 1 provides seamless data redundancy.*

Iomega's partner, Mozy, provides online backup designed to provide disaster recovery for small businesses. With MozyPro, you can easily backup your data over the internet to secure data centers. Mozy offers 24/7/365 onsite monitoring and security, state-of-the-art fire suppression systems, and seismic safeguards that can withstand a 7.5 magnitude earthquake. Redundant power distribution units and diesel generators ensure that even in the worst of circumstances, your data is protected. Good online backup systems provide multiple restore options. With MozyPro, you can either restore data quickly right from your computer in case of human error, or you can access your data remotely, from a web interface in the event of a more serious situation preventing you from accessing your business PC. In addition, you can request a DVD with your data delivered via FedEx for a small fee.

5. Backup systems need to be tested. Once you set up your backup and disaster recovery scheme, test it. Run a sample recovery – in some cases, as easy as restoring a file with another name. Taking a few moments to test the backup systems will provide great peace of mind, and prevent nasty surprises in a genuine shutdown or data loss situation. Check your backups at least monthly – ask your self again, how long could your business survive without access to critical data.

Continuously protecting and quickly recovering business-critical information is no longer optional. It is mission critical for any competitive organization, large or small.



Copyright © 2009 Iomega Corporation. All rights reserved. Iomega, ScreenPlay, and the stylized "i" logo are registered trademarks of Iomega Corporation in the United States and/or other countries. EMC and Retrospect are registered trademarks of EMC Corporation in the United States and/or other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Apple, Macintosh, and Mac are either registered trademarks or trademarks of Apple Inc. in the United States and/or other countries. Certain other product names, brand names, and company names may be trademarks or designations of their respective owners. 031809a