

WHITE PAPER



Data Disaster Recovery for Small and Medium Businesses

Table of Contents

Executive Summary	3
Business Objectives	4
Step 1 - Prioritization of Business Processes	4
Step 2 - Determine Business Objectives	5
Step 3 - Data Loss Scenarios	6
Step 4 - Identifying Recovery Objectives	7
Determining a Solution	8
Online Backup Addresses the SMB	8
Conclusion	10

EXECUTIVE SUMMARY

Businesses of all sizes have become increasingly dependent on data for the very existence of the company. Whether it is a large financial institution with transactional data or a 15-person law office with valuable client records, business assets are increasingly represented in the form of the data we maintain.

The business risk of losing this data or losing access for an extended period of time is well documented and for the most part, well understood. As evidence, a recent report from Gartner Group indicates that server backup in the Small and Medium Business (SMB) world is approaching 100%. And recent regulatory requirements are causing businesses to re-examine current recovery plans.

There is also an increasing awareness that responsible business protection also includes moving data to a safe offsite location. Certainly there are large-scale disasters such as hurricanes and tornados. However, to the businesses they affect, greater risk exists in the less publicized, but equally damaging events such as fire, flood, theft, a malfunction in the sprinkler system or simple human error.

But understanding the need is only the first step in the process. Equally important is determining the right data protection strategy for your business.

Data disaster protection comes in many shapes and sizes. What's best for a large global company may not be right for your business. Developing your data protection strategy does not have to be complicated, but it does need to be carefully thought out.

Proper planning requires clear answers to several critical questions, and the questions are the same regardless of the size of the business:

- **What functions of the business are imperative to generating revenue?**
- **What functions are imperative to normal operations?**
- **Which functions are less imperative, but still important to the business?**

The answers to these questions help determine minimally acceptable timeframes to recover from a failure and how much data loss is acceptable.

As individual SMB enterprises stop addressing data protection in generalities and start putting real timeframes and assigning real priorities to specific functions, the need for practical, affordable disaster recovery solutions becomes clearer.

Online backup and recovery is one solution that continues to gain significant market adoption within the SMB market. It provides the most cost effective and efficient data protection for Recovery Time (minimally acceptable time to recover from a loss) and Recovery Point (minimally acceptable data loss) objectives while solving the problem of backup and recovery, offsite data protection and the significant IT management and overhead that goes with each of those tasks.

BUSINESS OBJECTIVES

A recently published article by *InfoWorld* had the editor describing the value of her laptop as “\$2 million.” Is this outrageous? Absolutely not. The value of data as a business asset does not correlate to the medium that stores that data. If it did, the value of a Monet would equal the price of the canvas.

Business information—the information required to run a business—increasingly exists on server hard drives within computers. To adequately plan to protect that data, it is imperative for businesses to look not only at the value of the data on those systems, but also at the time required to get that data back after a failure and the tolerance for data loss after an event.

STEP 1 – Prioritization of Business Processes

The first step in planning a data protection strategy involves taking a critical look at the business and how it functions. Over the past three decades, computing infrastructure and the data that it manages has been completely integrated into the daily operation of most organizations. How long can an organization continue to operate without its infrastructure or its data?

Inevitably, your computer systems will fail. Determining the business value that data represents to your company is essential in order to plan recovery

of that business data when failure occurs. Fortunately, the value of data tends to align with function. Table 1 presents a possible categorization strategy that can be used in determining the value of systems in your organization. This table is a useful guide, but the content will vary by organization.

Faulkner Information Services indicates that 50 percent of businesses that lose their data due to disasters go out of business within 24 months and, according to the US Bureau of Labor, 93 percent are out of business within five years.

TABLE 1

IMPACT ON BUSINESS	TYPICAL BUSINESS FUNCTIONS	SAMPLE APPLICATIONS
Mission Critical	Revenue producing or customer facing	EDI, commerce, customer support...
Business Critical	Cross-organization operations	Back-office applications, email, manufacturing, supply chain
Operationally Important	Departmental	Departmental database, file server, print, HR management, data mining

How a company segments and ultimately prioritizes its business applications is highly dependent on individual business requirements. One organization may determine that email is a mission critical application while another may deem it far less critical. Consider the overall business impact of one of your systems being unavailable for an extended outage. What is the effect? Or consider the impact of re-entering data that may be lost in an outage. How much data is irreplaceable? These realities will drive your requirements for recovery objectives at the business application level.

Determining priority should be a process that is shared by executive management. The details must be addressed with the stakeholders of the business, where awareness must be built, defined and agreed upon. Only then can the process meet expectations.

STEP 2 – Determine Business Objectives

Once you have established the relative priority of business applications, it is possible to determine objectives for recovery. There are three primary concepts that need to be considered when planning a recovery strategy: Recovery Time Objective (RTO), Recovery Point Objective (RPO) and the scope of the Data Loss Event (DLE).

PLANNING CONCERNS	ACRONYM	DESCRIPTION
Recovery Time Objective	RTO	The time objective to bring a system back online following a failure
Recovery Point Objective	RPO	The acceptable amount of data loss since the last good backup prior to the point of failure
Data Loss Event	DLE	Type and scope of failure scenario that results in data loss

These concepts have been well integrated into the sound business practices of large enterprises. Now they are gaining significant attention in the small to medium enterprise. In addition, a series of market dynamics have made comprehensive data asset protection much more economical to smaller companies.

These changing dynamics include:

- A radical reduction in the cost of disk drive technology**
 ATA disk drives have had a significant impact on disk storage costs. IDC predicts that by 2006, ATA disks will be the number one drive technology within the enterprise
- Increased broadband penetration into SMB**
 Many small and medium businesses now have broadband of one kind or another and are looking for better ways to leverage that network connectivity
- Ever increasing management costs associated with storage management**
 Management problems associated with storage systems often cost six to nine times the system purchase price

Setting RTO and RPO goals requires the organization to look inward and make some clear, rational determinations as to how critical each business application is to the running of the company. Many businesses find that all data is not created equal. The nature of the industry, the organizational culture and the systems in place will all significantly affect these decisions and the resulting RTO, RPO and DLE standards.

Some real-world examples will help cement these concepts.

Example 1: A law firm with 100 attorneys determines that, in the event of a system failure, it is acceptable for client files to be inaccessible for 48 hours (Recovery Time). However, since the attorneys input data directly into the systems rather than on paper first, near zero data loss is acceptable (Recovery Point).

Example 2: A \$50 million insurance agency, whose business is dependent on being available to its customers when a disaster strikes, experiences a flood that causes widespread damage throughout the community. The agency must be back online processing customer claims in 4 hours (RTO). However, the agency's client interactions have a front end paper trail, so re-entry of a small amount of data prior to the failure is acceptable, a 2 hours RPO.

STEP 3 – Data Loss Scenarios

Data loss events come in various shapes, sizes and scopes. IT plays an important part in every disaster recovery plan, but by no means the only part. This is especially true when the disaster rises to the level of a site-wide or regional disaster where the entire business facility is inaccessible. In these situations, the data processing aspects of the business need to be addressed in the larger context of business recovery.

For example, a business will respond differently to a database corruption and a building fire. Although a fire is a rare event, the business recovery entails a vastly different scope (employee safety, new facility, communications, etc.) than a purely data-driven event such as a corrupted database.

While, taken alone, it may be critical to recover from a database corruption in 4 hours (RTO), if the business is recovering from a fire, the first four hours are usually dedicated to people and to securing a new place of business. So in this scenario, a four-hour RTO for a database is irrelevant. There is nowhere to recover that data to.

ESG Research has found that most companies cannot tolerate more than four hours of downtime before it has a serious affect on their business.

The scope of a data loss event affects not only the way a company responds, but also how much a company invests in protecting against the event. For a perspective on how frequently the most common types of data loss occur, refer to Table 2. Disaster recovery planning should address recovery requirements for all relevant types of data loss.

TABLE 2

TYPE OF LOSS	DESCRIPTION/EXAMPLES	FREQUENCY
File – Human Error	Human error, deletion, overwrite, data entry error, ...	83%
File – Corruption	File corruption, contained virus, application error, ...	10%
Storage Loss	Failure or loss of primary storage, e.g. corrupt RAID controller, etc.	5%
Server	CPU failure, storage RAID failure, theft, catastrophic virus	<1%
Site	Site disaster	<2%

STEP 4 – Identifying Recovery Objectives

At this point, the business has looked inward, determined the needs of business functions, prioritized business applications, identified data loss events and begun to define RTO and RPO goals. Now is the time to put all these concepts together and develop a simple chart identifying recovery objectives (RTO and RPO) for each class of application relative to the scope of the data loss event.

The following chart provides an example. The data is illustrative only.

RECOVERY OBJECTIVES (HYPOTHETICAL SCENARIO)

CLASS	PROTECTED	RTO	RPO
CLASS 1 MISSION CRITICAL			
File	Y	4 hrs	15 min
Storage/server	Y	24 hrs	15 min
Site	Y	48 hrs	15 min
CLASS 2 BUSINESS CRITICAL			
File	Y	8 hr	30 min
Storage/server	Y	48 hrs	30 min
Site	Y	3 days	30 min
CLASS 3 OPERATIONALLY IMPORTANT			
File	Y	8 hr	30 min
Storage/server	Y	48 hrs	30 min
Site	Y	4-5 days	30 min

IT professionals must keep several key points in mind as you develop your company's chart:

Correlation of objective to risk – Remember, not all Data Loss Events (DLE) are equally likely to occur. Consider the cost trade-offs when developing objectives.

Corporate buy-in – Executive-level business management support is imperative. These requirements and objectives must satisfy the business stakeholder so, without management buy-in, IT's ability to finalize an actionable plan is at risk.

Representing business value – Ensure that the recovery objectives represent the true business value of the data, including opportunity costs. Do your objectives account for the lost revenue when critical systems are down? Are they in line with the reality of recovering from a site loss?

Budget – The business case will eventually have to be made that these objectives and their subsequent costs are aligned. In many cases, but not all (a notable exception, online backup, is described below) the cost associated with recovery objectives increases as the acceptable time frame decreases.

Reality check with other recovery plans – It is generally good practice to do one last reality check to confirm that the IT recovery plan fits within the overall business recovery plan. An RTO of 1 hour in event of a site disaster does little good unless there is also a plan to have a correctly configured server in a computer room with communications gear and operators to run it in a shorter period of time.

DETERMINING A SOLUTION

Large enterprise organizations have been addressing these concepts and issues effectively for decades. But SMBs, equally dependent on data to run their businesses but not equally resourced, are only just now grappling with these issues and their ramifications. Instead of having an entire committee or even a single person to address the task, SMBs have an already stretched IT department that often looks at recovery planning as just one more thing that has to be done with no time or resources to do it.

While the planning and recovery tasks are similar for all enterprises, the needs of the SMB are different in many ways from that of the larger enterprise. By nature, SMBs are ultimately concerned with:

Ability to address RTO and RPO – It's always a priority to get systems back online and minimize data loss. But every organization's tolerance for delay and loss is different. Recovery Time/Recovery Point standards must be appropriate to your organization's particular needs.

Addressing All Data Loss Events (DLE) – The effect of unrecoverable data is too devastating to ignore. Therefore, all potential Data Loss Events must be identified and planned for, even if the likelihood of the event occurring is low. While the cost of rapidly recovering from some DLEs may be particularly onerous, planning enables the organization to rationally adjust Recovery Time and Recovery Point standards to offset costs.

Limited IT Resources – The reality is that IT resources are thin and adding additional tasks to under-resourced organizations often causes something to break.

Tight Budgets – Ideally, every company would want to have a fully redundant datacenter that can handle a fail-over of the entire business instantly. But this very expensive solution is just not practical for most SMBs.

Simplicity – Complexity is the enemy of thinly stretched resources. The ideal solution to the problem would solve the entire problem, achieve all objectives and not require burdensome ongoing management.

ONLINE BACKUP ADDRESSES THE SMB

Online backup and recovery is a solution to this problem that is gaining tremendous market acceptance within small and medium businesses. Online backup and recovery is the process of automatically moving data over the network from its primary servers to offsite storage located within a hardened electronic vault. This data is then available to be restored either over the network or through delivery of a network attached storage (NAS) device containing the recovered data.

Online backup is gaining momentum because of its ability to very simply cover the vast majority of business requirements at exceptionally affordable price points. In addition, recent trends in declining storage costs and availability of broadband network access have enabled large-scale market adoption of this technology.

Online backup is gaining momentum because of its ability to very simply cover the vast majority of business requirements at exceptionally affordable price points.

The advantages of online backup are many, but can be simplified into the following categories:

Fast RTOs – Network recovery of files and entire servers can be efficiently delivered from a simple web browser interface. In many scenarios, Recovery Time is effectively zero – meaning immediate return to business operations – and greatly improved when a complete recovery from offsite storage is necessary.

Instant offsite data protection – Data is moved offsite continuously, providing near zero data loss and very short RPOs.

Assured data recovery – It is no longer a secret. Often the data on backup tapes is unrecoverable. Independent analysts confirm that over 50% of all recoveries will fail because of errors in the backup process. By comparison, some online backup vendors offer a Service Level Agreement assuring reliable data recovery in the event of a disaster.

Remove burden of data protection – The initial purchase price of storage infrastructure is often dwarfed by the ongoing cost associated with the management and maintenance of that storage. A primary contributor to that cost is manual backup and recovery. Online backup and recovery is a completely automated, network delivered service that requires no ongoing monitoring or management by internal IT staff.

Professional management – Online backup includes 24 hour monitoring by online backup and recovery experts who proactively contact you if there's a disruption of your backup process caused by power loss, system failure or other unexpected event.

Recovery from anywhere – With online backup, the recovery can be initiated using a simple web browser from anywhere in the world. Traditional backup is manual and requires that the recovery be initiated at the server itself, eliminating the opportunity for remote recovery.

Cost effectiveness – Online backup is a managed service, saving SMBs the cost of hardware, software and annual maintenance. Personnel costs, measured in time saved, are also reduced, enabling your scarce IT resources to focus on more strategic activities.

Not all online backup providers offer the same level or type of service. To solve the problems of business data asset protection, be sure to compare the following attributes of online backup providers:

TABLE 4 – ONLINE BACKUP PROVIDER CHECKLIST

FEATURE CAPABILITIES	BUSINESS BENEFITS
Frequency of Backup	If returning to business with current data is an objective, the frequency of backup is critical. Continuous protection provides RPOs of minutes while with nightly batch backups, you're likely to lose at least 24 hours worth of data.
Service Level Agreements	Some providers specify assurance for data recovery in the SLA while others make no promises that the data is recoverable.
Remote Storage Facility	The storage location of your corporate data is critical. Only the most dependable names in data protection should be trusted.
Fully Managed Service	A fully managed service should require no reading of logs or monitoring of any kind by SMB personnel. These tasks add to the cost of ownership and offer many opportunities for errors. The service should provide 24x7 monitoring of service operations by backup and recovery experts.
Service Accessibility	Options range from fully web enabled where the service is accessed simply from web browser, to more complex solutions that require VPNs and remote security setups to access the server being protected.

CONCLUSION

Business management no longer questions the value of IT systems and the data contained within. Business managers do, however, expect their IT department to ensure that those systems are properly protected so the business is properly protected. Without foolproof data protection in place, every business is at great risk from the mundane damage caused by human error or a virus as well as the devastating damage of a flood, fire or total system failure.

As SMBs get more serious and systematic about disaster recovery, the responsibilities of IT professionals expand to ensure that the company can meet the prime business requirement after a data loss: timely recovery of systems (Recovery Time Objective or RTO), with current, usable data (Recovery Point Objective or RPO). And that must be accomplished while keeping in mind the dynamics of different Data Loss Events (DLE). Solutions abound, but the relevance and costs to a specific company must be closely examined.

Small and medium businesses are increasingly aware of these problems as customer expectations and market conditions change. And they are equally aware that complexity, cost and additional management responsibilities are things that the majority of IT shops don't want and just cannot take on.

Thankfully, online backup is a solution that addresses these problems, specifically as they relate to the SMB. Online backup is rapidly gaining acceptance and delivering levels of service that were, until recently, only available to the large enterprise. Online backup has the ability to greatly enhance an SMB organization's ability to meet RTO and RPO objectives at cost points that are usually lower than the traditional backup solutions already in place.

Disclaimer: This white paper may be redistributed in its entirety provided that the copyright notice is not removed. It may not be sold for profit or used in commercial documents without the written permission of the copyright holder. These documents are provided "as is" without any express or implied warranty. While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by Iron Mountain. The listing of an organization does not imply any sort of endorsement and Iron Mountain does not take any responsibility for the products or tools listed.

© 2006 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks and Iron Mountain Digital is a trademark of Iron Mountain Incorporated. All other trademarks are the property of their respective owners.



745 Atlantic Avenue
Boston, Massachusetts 02111
(800) 899-IRON

Iron Mountain Digital, the world's leading provider of data backup/recovery and archiving software as a service (SaaS), offers a comprehensive suite of data protection and e-records management software and services to thousands of companies around the world. For more information, visit our Web site at www.ironmountain.com/digital.