

Enterprise Data Protection and Recovery – The Why, The How, and Who To Go To

THE DRIVING FORCES TO PROTECT CRITICAL BUSINESS DATA

Data: A Fact of Business

We live in the information age. Even the smallest businesses rely on some type of computer systems to store the data — or information — they generate. This could be a list of customer phone numbers, a transaction log, or even details about a new product. If destroyed, damaged, misplaced, or stolen, this data could affect business operation. Examples of this critical data include:

1. **Intellectual property** — This is often a company's core competency. For example, in the case of a biotech firm, it is the need to access data captured in a discovery process; for a market research firm, it is access to database records.
2. **Private or sensitive data** — Examples range from scanned patient x-rays, credit card numbers, employee payroll information, etc.
3. **Vendor data** — This ranges from data about where an organization purchases supplies to build products to information about who is responsible for the delivery of products to customers.

Much data (over 60%) is decentralized and outside of centralized control. The mobilization of technology is leading more critical information beyond the protection of the data center. No longer do companies need to worry about just the data center. Now they need to make sure data from all sites is being backed up to standard processes and policies. Remote servers, PCs, and laptops all contain business critical and sensitive information that needs to be protected. Plus, employees can now log into networks through the Internet, which also leaves that data vulnerable to unauthorized access, so appropriate security measures need to be in place.

Because of the public's perceived increase in corporate corruption and stolen personal information, the federal government has reacted by instituting regulations to mandate the protection of sensitive data. Additionally, with state legislation requiring companies to disclose instances of stolen private information, companies should now be protecting backup data being physically moved off-site.

An effective data protection strategy not only restores data that has been destroyed, damaged, or misplaced but also prevents data from falling into the wrong hands as well as ensures that companies are in compliance with regulations affecting their industries.

The key for any organization — regardless of its size or the industry in which it plays — is to implement a data protection program that mitigates business risks, reduces costs, increases compliance, and helps improve overall business service levels.

DOCUMENT INFORMATION

Data Protection and Recovery — The Why, The How, and Who To Go To

PRINTED

April 2006

COPYRIGHT

Copyright © 2006 Iron Mountain Incorporated. All Rights Reserved.

TRADEMARKS

Iron Mountain and the design of the mountain are trademarks or registered trademarks and DataDefense is a trademark of Iron Mountain Incorporated. All other trademarks and registered trademarks are the property of their respective owners.

CONFIDENTIAL AND PROPRIETARY INFORMATION OF IRON MOUNTAIN. The information set forth herein represents the confidential and proprietary information of Iron Mountain. Such information shall only be used for the express purpose authorized by Iron Mountain and shall not be published, communicated, disclosed or divulged to any person, firm, corporation or legal entity, directly or indirectly, or to any third person without the prior written consent of Iron Mountain.

DISCLAIMER

While Iron Mountain has made every effort to ensure the accuracy and completeness of this document, it assumes no responsibility for the consequences to users of any errors that may be contained herein. The information in this document is subject to change without notice and should not be considered a commitment by Iron Mountain.

TABLE OF CONTENTS

Page

Reduced Risk, Reduced Cost, Increased Compliance	4
DATA PROTECTION FOR RECOVERY PURPOSES	4
Effective Data Protection and Recovery Strategy	4
Six Steps to a Complete Data Protection Strategy	4
Organize and Determine the Scope	5
Assess the Risks	5
Develop a Data Protection and Recovery Program	6
Implement the Program	6
Manage and Enforce	6
Audit/Test	7
A Word about Encryption	7
Methods for Data Protection for Disaster Recovery	8
OUTSOURCING TO AN OFF-SITE DATA PROTECTION PARTNER —	9
WHAT TO LOOK FOR	
Company Reputation	9
Breadth and Depth of Services	9
Automated Media Tracking	9
On-line Account Access	9
Secure Transport	9
Container Vaulting	9
Individual Media Vaulting	10
Physical Security Controls	10
Environmental Controls	10
Employee Background Checks	10
SUMMARY	11

ABOUT IRON MOUNTAIN INCORPORATED

Iron Mountain Incorporated (NYSE:IRM) is the world's trusted partner for records management and data protection services. Founded in 1951, the Company has grown to service more than 235,000 customer accounts throughout the United States, Canada, Europe and Latin America and the Pacific Rim. Iron Mountain offers records management services for both physical and digital media, disaster recovery support

services, and consulting — services that help businesses save money and manage risks associated with legal and regulatory compliance, protection of vital assets, and business continuity challenges. The DataDefense™ application is a complete encryption and security solution that is both simple to administer and user transparent, and will automatically eliminate data on lost or stolen computers.

For more information visit www.ironmountain.com

REDUCED RISK, REDUCED COST, INCREASED COMPLIANCE

Risks come in all shapes and sizes. In the IT world, risk mitigation is generally synonymous with data availability, internal/external security, and regulatory compliance.

When data is not protected properly, businesses can rack up a lengthy list of “hard” (e.g., fines levied on an organization in an electronic discovery suit, etc.) and “soft” (e.g., missed business opportunities) costs. An effective data protection strategy is able to minimize these costs by ensuring that data is available to those who need it (and are authorized to access it), when they need it, and according to business objectives.

Regulatory compliance adds another layer of IT risk. Businesses today must contend with an increasing number of government and non-government regulations. For example, organizations who store medical information are subject to the Health Insurance Portability and Accountability Act (HIPAA), financial organizations must address Security and Exchange Commissions (SEC) 17a-4 rule requirements, and industries of all types are accountable to Sarbanes-Oxley (SOX) stipulations.

The risks of non-compliance are serious and can include fines (often in the hundreds of millions of dollars), prosecution (of key corporate officers), or loss of business (forced to shut down).

DATA PROTECTION FOR RECOVERY PURPOSES

Effective Data Protection and Recovery Strategy

The reason to backup data is to be able to recover that data in the event of a disaster, failure, or loss. A data protection strategy should focus on minimizing risk to that data by getting it off-site, offline, and out-of-reach. Doing this keeps it secure and prevents it from falling into the wrong hands — which has become a large issue for both centralized and decentralized information. Backing up and protecting data also supports specific compliance objectives for different data types and different industries. Lastly, the strategy needs to encompass all critical data in order to support both centralized and distributed environments. More and more companies utilize a mobile and remote workforce, creating a greater geographic dispersion of data. It is not only imperative to understand where all the critical and sensitive information resides, but to make sure it is backed up consistently and securely in order to recover.

Data availability is a key issue today. Many businesses today demand 99.9999% uptime, or close to it. In other words, they require that users — and business applications — have access to critical information 24 hours a day, 7 days a week, 365 days a year (24x7x365). In this environment today, unplanned data outages can have a serious impact on the business operation. A solid data protection strategy ensures accessibility and availability of that data whenever and wherever it is needed, to get the business running again.

The consequences of not being able to access data when needed can be serious and include lost revenue. Worse still, news of these types of events, if made public, can have far-reaching consequences on all parties involved, affecting brand names and reputations.

Six Steps to a Complete Data Protection Strategy

A comprehensive data protection strategy encompasses a six-step process:

1. Organize
2. Assess
3. Development
4. Implement
5. Manage
6. Audit/Test

Organize and Determine the Scope

During the organization phase, it is important to not only understand where all the data is located but to make security the overall focus within all of IT and not just sections of it. Also, be sure to identify roles within the organization so people know who is responsible for doing specific tasks within the program.

While identifying roles, think about the process and separate duties where data is highly sensitive — doing this will help provide a multi-layered security approach to data access.

Assess the Risks

Know where all sensitive data resides, both centralized and distributed. Perform a risk analysis of the entire backup process and examine each step of the backup methodology, looking for security holes. Are containers left out in the open? Can backup tapes be secretly copied? These areas of concern need to be identified and fixed. If a risk analysis exposes numerous vulnerabilities, where unauthorized access is possible, the organization should seriously consider the cost of encryption. Of course the total cost of encryption should be compared to the risks and likelihood of stolen data and the potential hazards for the company.

Additionally, companies need to assess their data and tier it according to the value it has to the business. For example, business critical data should reside on high performance storage and have more stringent backup and protection policies, where as less valuable data that is not business critical or subject to Government regulations can be stored on inexpensive tape media, with less stringent backup and protection policies.

For simplification purposes, data in any organization can be categorized into five classes, each of which should be protected differently.

Class	Description
Class I — Urgent business critical or mission critical data	The data that must be online and available at all times. If this data is corrupted or becomes unavailable, it will result in significant loss of revenue or disruption of services
Class II — Non-urgent business critical data or essential data	This data is required for the day-to-day running of the business. However, a small disruption in availability of this data will not result in loss of revenue or disruption of services provided by the company.
Class III — Current non-critical data	This is data generated by the day-to-day business processes. Disruption in availability or some data loss will not result in loss of revenue or disruption of services provided by the company.
Class IV — Non-current data	This is the same as current non-critical data (Class III), but only includes files that have not been accessed within the last 90 days.
Class V — Legally required data	This is data that the company is legally required to retain but does not need to be kept online.

DEVELOP A DATA PROTECTION AND RECOVERY PROGRAM

When developing a program, adopt a multi-layered approach that may already exist for the data network, and apply that ideology to the storage network, while adding layers that are characteristic to data at rest:

- **Authentication** — Apply multi-level authentication techniques
- **Authorization** — Enforce privileges based on roles and responsibilities
- **Encryption** — All sensitive data should be encrypted when it is stored or copied
- **Auditing** — Logs of administrative operations by users should be maintained for traceability and accountability

Depending on a single copy is never a good idea. A good practice is to perform nightly backups and then ship copies of those tapes off-site with a trusted third-party so they are protected and available for recovery in the event of a disaster. Getting the media off-site will protect it from unauthorized access and potential tampering.

A tight end-to-end chain of custody is essential to knowing where your backup media is at all times. For removable media, a best practice is to use bar codes and generate daily reports for media being sent off-site and those that need to be returned. Media should be scanned at specific intervals of the movement process and placed in locked containers during transportation. Be sure to reconcile the media stored off-site on a regular basis with tapes kept in house and any discrepancies should be addressed.

More and more critical business data resides not only at remote offices, but on PCs and laptops. It is absolutely critical to backup this data and protect it. Most remote sites do not have dedicated IT staff, leaving the backup process full of holes because it does not happen regularly, is typically incomplete, and no one knows where the backed up data is stored. All these issues leave the data vulnerable to unauthorized users, theft, and the inability to fully recover. Be sure to review technologies like electronic vaulting that provide a secure, consistent, and automated solution to backing up and protecting distributed data.

Lastly, once media reaches a point of uselessness, that media must be properly destroyed. This includes scrambling, degauzing, and even pulverization. Destruction is best performed by a third party that can provide a certificate of destruction.

Implement the Program

Once the plan for a complete data protection and recovery program has been developed, it needs to be implemented. More importantly the process needs to be communicated throughout the organization.

Data loss and information theft are a business issue, not an IT issue. Therefore a program to educate executives, as well as all employees, on risks, threats, and potential losses from data theft should be conducted. Additionally, the educational effort should include the costs to defend data against unauthorized access. With this information, corporate officers can make knowledgeable decisions on cost/benefit profiles for complete backup data protection.

Manage and Enforce

Implementing a program is only half the battle. Once it's up and running you must have consistent methods in place to enforce it. You need to make sure it stays up to date and that employees are continually reminded of their role so that it becomes second nature for them. And you have to budget for program maintenance, testing, and enhancement.

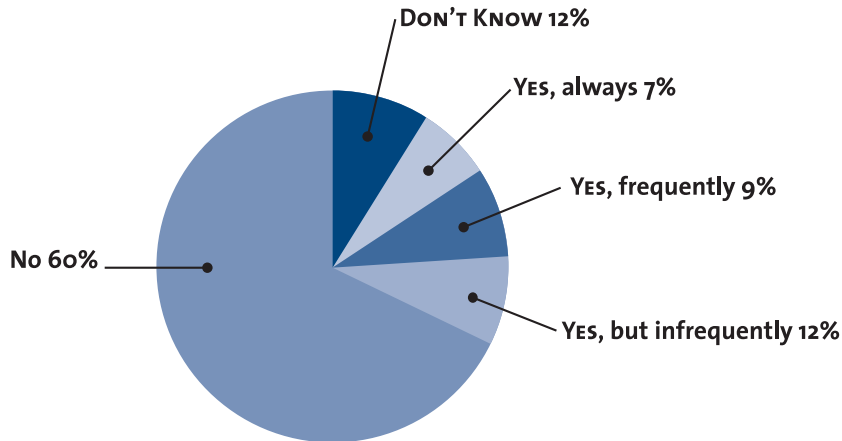
Audit/Test

Be sure to test the process once it is in place. Remember to test not only the backup but also the recovery and put the plan through its paces. Try to inflict various threats to the process such as device issues, data classification issues, and any other scenario that could affect the business. Also test using people less familiar with the process which will help ensure it is easy to follow and can be done by others if the usual personnel are not available. Be sure to run through a simulated disaster event once a year to ensure recovery procedures are sound. Be flexible and change the program as the needs of the business change.

A WORD ABOUT ENCRYPTION

Almost all companies back up their data regularly and maintain copies off-site for data retention and disaster recovery protection. Although many backup tapes contain sensitive information and are often physically transported off-site, most companies do not encrypt their backup tapes. According to a recent ESG survey, sixty percent claim their companies never encrypt their backups. This lack of encryption is even true in “security-conscious” industry sectors like financial services (65% never encrypt backups), government (77% never encrypt backups), and healthcare (67% never encrypt backups).

Does your company encrypt data as it is backed up to tape?
(PERCENT STORAGE PROFESSIONALS)



MARCH 2005

SOURCE: Enterprise Strategy Group

Backup encryption continues to be avoided because many IT professionals maintain erroneous beliefs about encryption technology: that is building an end-to-end security infrastructure will take years to complete. This assumption is compounded by the lack of backup encryption, despite the fact there are a number of proven solutions available to solve that issue. Here are three types:

1. Application/Database encryption: Database applications offer both native and third-party tools that can encrypt sensitive tables to ensure that data is viewable only by users specifically authorized to see those elements. Data elements such as credit card numbers, employee salary information, and personal medical data are often encrypted in this way. The advantage of application-based encryption is that it is tightly coupled with the application itself. It encrypts only the data that needs to be encrypted. It also has the advantage of encrypting data at its origin, providing an even greater level of security.

2. Operating system encryption: Modern operating systems also incorporate the ability to encrypt data stored within a file system, directory, or individual file. For example, Microsoft® Windows® XP provides an Encrypting File System that supports public key encryption, and is fully integrated with the operating system. Encryption at this level can be very flexible and applied to a wide range of data. The potential downside is CPU overhead and file system performance as data must be decrypted to be accessed.
3. Network encryption devices: At the network level, a breed of hardware security modules (HSMs) have emerged that can provide a transparent level of data encryption. These appliances can sit on either a SAN or LAN and have several advantages that make them worthy of consideration. First, they are fast, performing at wire speed with minimal latency to the environment. Second, they are versatile, meeting the needs of a broad range of specific encryption requirements and network architectures. Third, network encryption devices are relatively inexpensive. Given the risk of privacy exposure or loss of proprietary information, the return on investment of these devices can be compelling.

METHODS FOR DATA PROTECTION FOR DISASTER RECOVERY

There are several methods for getting backup data off-site. The overall goal is redundancy of that data so that it can be restored in the event the original is unavailable due to deletion, loss, or disaster. While making backup copies of data is still the most common method of disaster preparedness, other technologies are quickly gaining popularity.

1. Backup tapes are created for offsite storage by sending the original tape off-site; however, this can complicate day-to-day recoveries since the tapes are no longer available onsite. A better process is to copy the original backup to another tape and send that copy off-site.
2. Replicating, or making a mirror image of that data, at a second location. Replication is the practice of copying all files or blocks that have changed on the source system to a target system. Every time a file or block changes on the source system, that same file or block changes on the target system. Replication based backup is today often considered a key component for both backup and data protection.

But replication-based backup does have some issues:

- It replicates everything – the good, the bad, and the ugly (e.g., virus and file deletions). A replication based backup system, therefore, must be able to provide a history by either backing up the replicated destination or taking snapshots.
 - It is comparatively immature, compared to traditional backup-and-recovery software. For example, few replication products can interface with databases.
3. Continuous Data Protection Systems: A true continuous data protection (CDP) system is simply a replication-based backup system. Using either “push agent software” running on a server or “replication software” running within the network storage system, files that are changed on the source side are also changed on the destination side. However, unlike replication, CDP systems allow users to roll back to any point in time. In the event of a disaster or failure of some type, the IT manager would simply dial back the clock to a few seconds prior to the disaster.

CDP products can also be used to solve the problem of remote office and branch office backup. A CDP system like Iron Mountain’s Electronic Vaulting solutions that continuously backs up the remote office to a central backup system can provide a much better backup process that is automated and consistent.

4. Snapshots: A snapshot is a virtual copy of a device or file system. It is similar to a Windows shortcut to a device that has been frozen in time. Just as a symbolic link or shortcut is not really a copy of a file to which it points, a snapshot is not a real copy of the file system to which it points. The only difference between a snapshot and a shortcut, or symbolic link, is that a snapshot always mimics the way that file or device looked at the specific point in time (PIT) that the snapshot was taken.

OUTSOURCING TO AN OFF-SITE DATA PROTECTION PARTNER — WHAT TO LOOK FOR

An off-site data protection company, or vaulting company, will protect your backup media necessary to restore data in case of disaster. These vendors also typically protect archived media as well. Finding a good off-site storage company is important. Here is a quick list of some of the things you should consider:

Company Reputation

The last thing you need in the event of a disaster is an off-site vaulting company that is inexperienced or unprepared to support you in your time of need. Trust, security, and experience is paramount.

Breadth and Depth of Services

The partner should have the ability to offer services for a complete data protection strategy — for centralized and decentralized information, encryption and digital archiving. Also important is a national and international footprint to provide global consistency with locally implemented services, thus ensuring proper disaster recovery assistance.

Automated Media Tracking

The company's systems should be able to utilize existing barcode labels on your media as well as track all media in transport between you and the off-site location. This provides consistent, secure processes for handling and transporting media from start to finish that proves a chain of custody.

On-line Account Access

The partner should have a web-based customer interface, to provide complete, accurate, real-time visibility and control to your account — any time, any place. As a result, you can quickly and easily monitor and manage your media online to expedite your company's standard rotational practices, special media requests, maintain a disaster recovery plan, and manage the list of authorized personnel.

Secure Transport

Review and discuss the entire process of how your media is handled from start to finish. Look for an emphasis on physical security, scanning points, audit trails, and control mechanisms to ensure that the entire process is being followed.

Container Vaulting

Container vaulting is when you send a box of tapes, and only the box is tracked. Your selected vendor should support this type of vaulting, particularly for systems that send full backups in sets for one or more servers with a common retention period.

Individual Media Vaulting

Individual media vaulting is when you send a box of tapes, and each piece of media in the box is tracked. Your selected vendor should support this type of vaulting, including barcode scan verification of all incoming and outgoing media.

Physical Security Controls

It should be impossible for anyone to get in the vault. You should be able to get access to your media with proper identification, of course, but you should never be able to just go in the vault.

Environmental Controls

Tapes and other media should not be stored in a box in your car trunk, or any other non-environmentally controlled location. Your backup media should be stored in an environment that is strictly controlled, including temperature, humidity, and static control. This also includes isolating the media from other sources of contamination and providing gaseous fire protection systems (e.g., Halon, FM200, etc.).

Employee Background Checks

Your selected vendor is going to protect all of your critical data, so you must trust every one of their employees. Therefore, it is critical that employee background checks are performed routinely.

SUMMARY

An effective data protection and recovery strategy not only restores data that has been destroyed, damaged or misplaced but also prevents information from falling into the wrong hands. Additionally, a sound strategy helps ensure companies are meeting compliance requirements within regulations affecting their industries.

The key for any organization — regardless of its size or the industry in which it plays — is to implement a data protection strategy that mitigates business risk, reduces cost, and increases compliance, while helping to improve overall business service levels. Ensure your data is protected and quickly recoverable by outsourcing with a trusted partner having the expertise, resources, security, and consistent best practices processes.

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



120 Turnpike Road
Southborough, Massachusetts 01772
(800) 899-IRON

Iron Mountain Digital is the world's leading provider of Storage-as-a Service solutions for backup and archiving. The technology arm of Iron Mountain Incorporated offers a comprehensive suite of data protection, archiving and intellectual property management solutions to thousands of companies around the world, directly and through a worldwide network of channel partners. Iron Mountain Digital is based in Southborough, Mass. with European headquarters in Frankfurt, Germany.