

The Data Recovery Solution

A White Paper by ONTRACK Data Recovery, Inc.

Contents

Data Loss Dangers	one
Critical Data Risks	two
Challenges and Responsibilities	three
Protection, Detection, Correction	four
Finding the Optimum Solution	five
The Data Recovery Alternative	eight
When is Data Recovery Necessary?	nine
Data Recovery Case Studies	ten
Final Analysis	eleven
Additional Information	eleven

Ontrack[®]

Defining Data Recovery Solutions Worldwide

6321 Bury Drive
Eden Prairie, MN 55346
612-937-5161 • 1-800-872-2599
www.ontrack.com

©1998 ONTRACK Data International, Inc.

The Data Recovery Solution

- A RAID system's cooling process collapses, causing its drives to overheat and fail.
- A company attempts to restore lost data from carefully collected backups, only to discover the backups are unreadable.
- A business adds a drive to its NetWare server, accidentally erasing the server's partitions.
- An MIS administrator completes a fix on a mirrored drive without shutting off the mirror, losing the reference point for the original data.

Data loss disasters like these are becoming increasingly commonplace. This is due, in part, to rapidly changing computer technologies. As drives get smaller and smaller, drive heads come closer and closer to the rotating media. The results are more frequent equipment failures and more destructive data losses. The increase in data disasters also stems from the sheer volume of data generated by modern companies and the decentralized way that data is produced, collected, and stored. As distributed network models proliferate, and organizations continue to open their doors to the Internet, threats to data integrity and data security are compounded.

While data backups would seem to offer an effective shield against these threats, backups do not always provide comprehensive data protection. That is because the data backup plans developed by many companies are not fully realized or, worse yet, not followed. What is more, individuals often fail to test the "restore" capabilities of their backup media. If the backups are faulty, a simple data loss can quickly become a data disaster. Finally, even if backups are successful, they only contain data collected during the most recent backup session. As a result, a data loss can potentially rob you of your most current data, despite your backup attempts.

The reality of data loss forces business executives to ask themselves some serious questions. For example: Does a major data loss put your business interests at risk? Does data loss expose your company to legal repercussions? How susceptible are your data storage devices to corruptions and crashes? What can be done to properly protect and recover critical data?

The importance of computer data to the daily operation of your organization requires you not only to ask these questions, but to successfully answer them as well. This paper will help you in your effort to answer these questions.

Data Loss Dangers

.....
: *"If an organization is* :
: *fortunate enough to survive a* :
: *disaster without a plan for* :
: *recovery, it will not survive* :
: *unscathed. Aside from the* :
: *direct revenue losses* :
: *incurred during a failure, the* :
: *organization will also suffer* :
: *intangible costs such as cash* :
: *flow interruptions, loss of* :
: *customers, loss of competi-* :
: *tive edge, erosion of industry* :
: *image, and reduced market* :
: *share."* :
: DRT Systems White Paper :
:

Critical Data Risks

Computer data may be one of your company's most vulnerable assets. According to our experience in the ONTRACK Data Recovery professional labs, the primary threats to your data integrity are as follows:

CAUSE OF DATA LOSS	FREQUENCY OF OCCURRENCE
Hardware or system malfunction	44%
Human error	32%
Software program malfunction	4%
Viruses	7%
Natural disaster	3%

Source: ONTRACK Data Recovery, Inc., 1995-1996.

This data is based on the actual data recoveries performed by ONTRACK.

These five major threats to your computer data share two things in common: they are unpredictable and, in many cases, uncontrollable. Therefore, the precautions taken by IS executives to safeguard company data cannot always prevent a data loss disaster.

In addition to being a vulnerable asset, computer data is also a valuable asset. According to a Gallup Poll, most businesses value 100 megabytes of data at \$1 million. Using this figure as a starting point, it is easy to see how significant the costs of lost or inaccessible data can be. The following is a summary of the average hourly impact of lost or inaccessible data on a selection of different businesses.

TYPE OF BUSINESS	AVERAGE HOURLY IMPACT
Retail brokerage	\$6.45 million
Credit card sales authorization	\$2.60 million
Home shopping channels	\$113,750
Catalog sales centers	\$90,000
Airline reservation centers	\$89,500
Cellular service activation	\$41,000
Package shipping service	\$28,250
Online network connection fees	\$25,250
ATM service fees	\$14,500

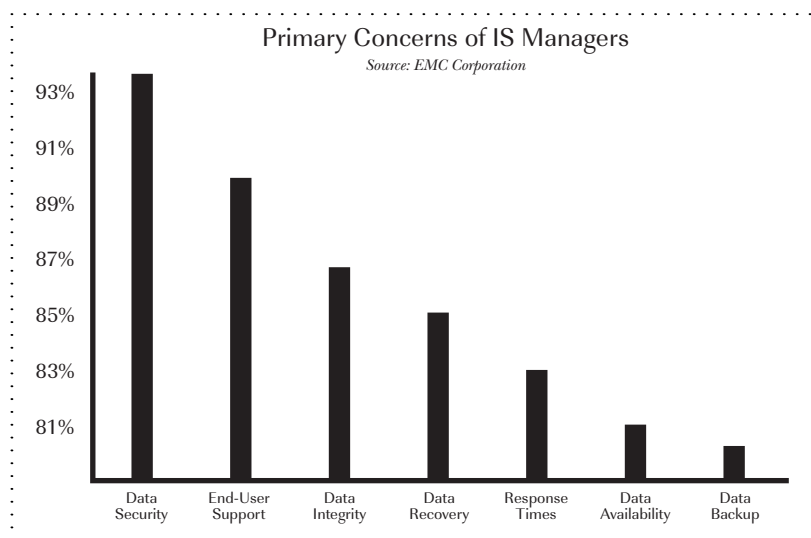
Source: Contingency Planning Research

While the financial importance of data integrity is clear to most business executives, less obvious is the legal importance of data integrity. According to "The Legal Issues of Disaster Recovery Planning" by Tari Schreider, there exist a collection of legal precedents that can be used to hold a company accountable to those people affected by that company's inability to cope with, or recover from, a disaster. In other words, a temporary or permanent data loss could unnecessarily expose your company to customer lawsuits and other related legal actions. Coupled with its financial costs, the legal costs of a data loss could put your company's future at severe risk.

Challenges and Responsibilities

As established in the previous section, lost or inaccessible data can have a devastating, if not fatal, impact on your company. In fact, according to Jon Toigo's "Disaster Recovery Planning," the average company experiencing a computer outage lasting more than 10 days will never fully recover financially. Furthermore, 50% of these companies will be out of business within five years. The need to avert the business costs associated with data loss provides today's IS executives with unique challenges and responsibilities.

The primary challenges and responsibilities faced by IS executives can be divided into three major categories. First, IS executives must effectively manage mission-critical data that is distributed throughout a company on a wide variety of platforms. Second, they must deliver the same level of stability, reliability, and security provided by traditional, mainframe-centric operations. And third, they must support the data management requirements of all company users, including the need to assist those users who experience a data loss.



Given the challenges and responsibilities they face, it is crucial that IS executives develop and follow a plan for maintaining data integrity and ensuring data security. In order for such a plan to be effective, particular emphasis must be placed on the three cornerstones of data integrity and security: **protecting** data, **detecting** potential data loss situations, and **correcting** data loss conditions before or immediately after they occur. Implementing the protection, detection, and correction model can help your company avoid the considerable costs in time and money of severe data loss.

Protection, Detection, Correction

“Rarely—almost never—do we talk to an executive who has not thought of disaster recovery. In most cases, though, they recognize the need to do something but not necessarily what to do.”

That quote, published in the August 14, 1995 issue of LAN Times, comes from Mike Symmers, manager of business recovery services for Chicago-based Anderson Consulting. In one single line, Symmers articulates the dilemma facing all companies and

their IS executives: What can I do to properly safeguard my data against disaster? The most effective answer to this question is **protection, detection, and correction**.

The protection, detection, and correction model can be summarized as follows:

Protection

Procedures and system configurations must be established in an effort to minimize the major threats to data integrity: hardware failures, human errors, software malfunctions, computer viruses, natural disasters, and computer crimes.

Detection

Risks to data integrity must be quickly and accurately detected before they adversely affect business.

Correction

The precursors to data loss must be corrected before a data loss situation materializes. If a data loss does occur, business downtime must be minimized, crucial data must be recovered, and appropriate business continuity plans must be implemented.

There are twelve primary ways to fully realize the data integrity and information security principles called for by the protection, detection, and correction model. Each of these methods is applicable to specific data protection needs and situations.

1. Redundancy: RAID (Redundant Array of Inexpensive Disks) systems—Two or more drives working together that provide increased performance and various levels of error recovery and fault tolerance.
Disk or system mirroring—Recording redundant data for fault-tolerant operation. During disk mirroring, data is written on two partitions of the same disk or two separate disks within the same system. During system mirroring, data is written to two separate computer systems.
2. Backup and restoration
3. Data re-entry
4. Off-site storage
5. Electronic vaulting—Automatic, remote copying and storing of critical computer data over high-speed communication lines.
6. Commercial software (anti-virus, data restoration)



7. Data protection consulting/site audits
8. Disaster recovery plans
9. Firewalls—A network node set up as a boundary to prevent unauthorized traffic from entering into a specific segment of the network.
10. Authentication software—Verifies a user is the person he or she claims to be.
11. Uninterrupted power supply (UPS)
12. Data recovery services—Restoring physically damaged or corrupted data from storage media. During data recovery, the data is recovered directly from the damaged media source itself.

Each of these options has its strengths and weaknesses, depending on the environment you are addressing, and the level of protection you desire. Therefore, for the most effective implementation of the protection, detection, and correction model, you must carefully consider which information security and data integrity options best suit your needs.

The problem with finding the perfect recipe for protection, detection, and correction is simple: common data security and integrity options (backup and restoration, data re-entry, RAID systems) are not the optimum solutions for all situations. For instance, there is the belief that having a mirrored or RAID system completely protects companies against high risk data loss. There is also the belief that a downed system can be instantly and completely resurrected from data backups. Unfortunately, mirrored and RAID systems fail, and backups can either be outdated or corrupted.

With this in mind, IS executives must understand not only their protection, detection, and correction options, but the advantages and disadvantages each option has to offer. The following chart explores these options and the recovery professionals can successfully augment the current protection, detection,

Finding the Optimum Solution

PROTECTION, DETECTION CORRECTION OPTION	STRENGTHS	RISKS
RAID systems	RAID can often provide 100% protection against downtime.	<ul style="list-style-type: none"> • RAID systems can fall victim to high risk threats, including power problems and human errors. • Two or more drives may fail at the same time, rendering your entire system unavailable.
Mirrored systems	Mirrored systems can provide adequate real-time backup of mission-critical data.	<ul style="list-style-type: none"> • Mirrored systems are exposed to many threats, ranging from incorrect system configuration to human error. • If the primary system is corrupted and then mirrored, your primary and mirrored systems are both corrupted.
Backup and restoration	By performing regular backups, data can be quickly restored, and business activities can be quickly resumed, after a data loss situation.	<ul style="list-style-type: none"> • Backups must be made completely and consistently if they are to be of any use. This is no easy task, considering that many networks operate 24 hours a day. • Tape backups can become corrupted or fall victim to human error. • Tape restoration retrieves data from the last backup, leaving a “gap” between old and new data. This “gap” necessitates data re-entry or re-creation, adding to the costs in time and money of data loss
Electronic vaulting	<ul style="list-style-type: none"> • Electronic vaulting can eliminate the hassle and error potential of manual and individual tape backups. • CD backups may present fewer opportunities for backup media corruption. 	<ul style="list-style-type: none"> • Restoring from electronic vaults may still have a restoration “gap” between old and new data. • Depending on where the vault is located, and how quickly your data can be retrieved, you may face the expenses associated with additional downtime.
Anti-virus software	Anti-virus software, when used properly, can provide constant protection against virus corruption.	<ul style="list-style-type: none"> • Viruses are created at an astounding rate. This means that anti-virus software must be consistently updated to remain useful and effective • An organization’s anti-virus policies are not always followed or are not as good as they could be for proper protection. • Many companies lack anti-virus plans.

PROTECTION, DETECTION CORRECTION OPTION	STRENGTHS	RISKS
Disaster recovery/business continuity plans	<p>These plans can provide the necessary procedures to help an organization resume vital operations and return to normal business functions as quickly as possible following a disaster situation.</p>	<ul style="list-style-type: none"> • Although they provide procedures on how to set up operations at a hot or cold site, disaster plans often fail to address data recovery concerns and options. • These plans emphasize major disasters, failing to address everyday incidents of data loss and data corruption. • People fail to update their disaster plans.
Commercial file recovery software	<p>File recovery software can provide the necessary tools to recover lost files.</p>	<ul style="list-style-type: none"> • In some cases, commercial software can provide a successful data recovery. However, there are instances when these utilities can aggravate an existing problem or fail to give the advanced tools needed for a complete data recovery. • Some commercial software products attempt to repair damage to a drive or volume before attempting to recover data. This can lead to additional data loss.
Data re-entry/restoration	<p>When files are lost or corrupted, data re-entry can be the easiest and most convenient way to resume normal business functions.</p>	<ul style="list-style-type: none"> • Data re-entry is not always the most efficient recovery method, especially when the value of time, money, and the data is high. • With users manually re-creating lost data, the data re-entry process is especially vulnerable to human errors.
Data protection experts (internal and external)	<p>An internal or external “expert” can help recover lost or corrupted data.</p>	<p>Individuals make the mistake of attaching the “expert” label to anyone who knows more about computers than the individuals do. This means that data recovery operations may be left in the hands of someone unqualified to properly perform the job. Not only does this put data at risk, it may lead to additional data loss, downtime, and expenses for the company.</p>
Data recovery services	<ul style="list-style-type: none"> • Data recovery service providers can successfully complete a full data recovery. • Data recovery service provides a fast turnaround time and quick restoration. • Data recovery restores your current data. • Data recovery services are cost-effective. 	<ul style="list-style-type: none"> • The capabilities of all data recovery companies are not the same. Because data recovery tools and techniques are typically developed “in-house,” and because some tools and techniques are more powerful than others, some data recovery companies are better equipped to provide a total recovery. • In the event of a massive disk drive crash, even a professional data recovery company may be unable to retrieve lost data.

The Data Recovery Alternative

While IS executives have had extensive experience with more conventional protection, detection, and correction tools like backup and restoration, data re-entry, and RAID systems, they are often unaware of the possibilities provided by professional data recovery services. Like the other protection, detection, and correction tools discussed in the previous section, data recovery does have its drawbacks. For instance, technological capabilities and staff expertise make some data recovery companies far better equipped than others to recover data. Furthermore, if an organization is unfettered by time constraints, and the data they lose is not central to continued business operations, professional data recovery services may be unnecessary from an economic perspective.

However, when time is crucial and data is mission-critical, data recovery may be the most practical option available. That is because data recovery professionals recover data from the damaged media itself, providing several advantages over alternative methods of data retrieval. First, professional recovery is **complete**. While many people use commercial software utilities in an effort to retrieve lost data, these utilities can often destroy what was otherwise recoverable information. Data recovery professionals can safely enter the system or media to achieve a comprehensive data recovery. Second, professional recovery services **recover current data**. Although many people revert to backups following a data loss, those backups typically contain outdated information. Third, professional data recovery service is **fast**. Every second that passes following a data disaster means time and money lost to your company. Professional service reduces this downtime by quickly recovering and returning your data. Fourth, professional services are **cost-effective**. The expense in time, money, and effort of rebuilding or re-keying lost data can be overwhelming to your company. Professional recovery services provide the quickest and most complete data recovery possible. Finally, professional services provide an extra level of **protection, detection, and correction**. These services can be used to augment a company's current data integrity and security procedures, or to assist a company that falls victim to a catastrophic loss.

- *The proportion of computing power allocated to LANs has doubled from 18% of capacity in 1993 to 36% in 1995.*

Computing Canada,
March 1, 1995

- *The use of LANs as a primary system has more than tripled from 8% in 1993 to 28% in 1995. 43% of all LANs now house mission-critical applications.*

Computing Canada,
March 1, 1995

- *It typically takes five days to recover a failed LAN.*

Infosecurity News,
Jan./Feb. 1995

- *20% of the time, data can be restored through data re-entry in less than one day. 40% of the time, restoration takes between two and five days. 40% of the time, restoration takes more than five days.*

Contingency Planning Research

- *Depending on the level of service and the situation, ONTRACK Data Recovery can completely restore lost data in one day or less.*

ONTRACK Data Recovery, Inc.,
1995-1996

When is Data Recovery Necessary?

In many instances, data recovery is not just the most practical protection, detection, and correction option available, it is the only option available. The following are examples of data loss situations during which professional data recovery services are essential to the safe return of your endangered data.

Data recovery is necessary when you lack a backup system.

Without the safety net of a dependable backup system, a data loss of any size could prove disastrous for your organization. In this instance, data recovery experts can utilize the appropriate tools and technology to recover your critical data.

Data recovery is necessary when your backup and restore system fails.

While typically reliable, your backup and restore process can be compromised by unreadable backups, corrupted backup data, and improper backup procedures. Furthermore, even if the backup is successful, there will be a time gap between the last backup session and the data loss. As a result, your current data will not be recovered and restored. In the event of backup failure, data recovery professionals can safely enter your system or media to completely recover your most recent data.

Data recovery is necessary when your mirrored system fails.

In order to safeguard critical business information, many organizations simultaneously copy data to two separate computer systems. If, however, that data is corrupted before it is copied, or if one or both of the two systems fail, your critical data may be irrevocably lost or destroyed. Data recovery professionals can rectify this situation by directly accessing the storage media itself to perform a swift and accurate recovery.

Data recovery is necessary when re-creation is impractical or impossible.

Data re-creation or re-keying involves a number of unseen costs that can make it an impractical, if not impossible, option. First is the cost in time. Not only is the re-keying process slow, it keeps employees from working on today's business. Next is the cost in money. A National Computer Security Association survey found that it costs nearly \$100,000 to rebuild 20 megabytes of data lost by an average engineering department. Finally, there is the cost in quality. Inputting lost data manually increases the chance for user error and threatens data integrity. In contrast, professional data recovery service can provide a fast, cost-effective, and accurate return of your data.

Data recovery is necessary when you fall victim to computer crime.

If your organization's data is intentionally stolen, altered, or destroyed, professional data recovery services can help. ONTRACK Data Recovery features a Computer Evidence Services division that can locate and analyze computer data evidence, and support you with expert testimony if your computer crime incident results in legal proceedings. In this and many other instances, data recovery service is the lone protection, detection, and correction solution available.

Data Recovery Case Studies

ONTRACK Data Recovery, Inc. has performed tens of thousands of successful data recoveries in a wide array of situations for a diverse group of corporate and individual clients, including Fortune 500 companies and the federal government. While each data recovery operation is unique, there are two case studies that have particular relevance to the discussion of the data protection, detection, and correction model.

The first study involves a database warehouse company responsible for storing crucial business information for outside firms. Between 6 p.m. and 7 p.m. on a Friday night, the company's RAID 5 system failed. According to the IS executive in charge, a monitoring utility indicated that one of the system's drives was going bad, but did not indicate that a second drive was also experiencing problems. When both drives failed, the company lost eight gigabytes of data.

.....
: "ONTRACK's service was tremendous.
: They did things I was surprised they
: could do. The service was a pleasant
: surprise."
:

: IS Executive
:

Because of the size of the data loss, the critical nature of the data, the importance of avoiding costly downtime, and the need to protect the company's reputation as a safe place to store data, the IS executive called ONTRACK for emergency data recovery services. The IS executive said he was not only surprised that engineers were available when he called ONTRACK late on a Friday night, he was also surprised at how quickly they provided a 100% recovery. With the help of ONTRACK, the database company was able to resume normal business functions in time for the new work week.

In light of the RAID failure, the IS executive made three changes to company policy. First, he instituted a more comprehensive tape backup program. Second, he hired an MIS employee whose sole duty it is to make tape backups and verify their integrity. And third, he developed a relationship with ONTRACK. With these three changes, the IS executive established a more effective protection, detection, and correction model for his company.

.....
: "It's nice to know there are profession-
: als out there who can really help.
: ONTRACK did an excellent job."
:

: Bob Kendall, Cole Publishing, Inc.
:

The second case study concerns Cole Publishing, Inc., a Wisconsin-based firm that produces specialty trade journals. When a hard drive crash caused the loss of more than 50,000 names from the company's subscription list, Cole was forced to resort to its most recent tape backup, recorded one week earlier. Unfortunately, attempts to restore from the backup revealed that the backup data was corrupted, and the only other backup the company had was several months out of date.

The president of Cole Publishing, Bob Kendall, quickly called ONTRACK to see if his company's data could be recovered. Because time was not as critical as the missing data itself, Kendall opted for ONTRACK standard data recovery service. Within five days, 99% of the lost data was recovered and restored.

Following this incident, Cole Publishing implemented regimented tape backup procedures in an effort to avoid future corruption. They also instituted a policy that any actual or potential data loss situation should be forwarded to ONTRACK. Much like the IS executive at the database warehouse company, Bob Kendall concluded that professional data recovery companies are uniquely qualified to recover data during a data loss situation.

While the two companies featured in the case studies realized the importance of the protection, detection, and correction paradigm, they did not realize it until it was too late. This underscores the emphasis companies must place on fully understanding the professional, financial, and legal implications of data loss, and proactively exploring the wealth of options available for maintaining data integrity and information security before data loss occurs. Preventing sustained downtime and devastating data loss is the ultimate goal of all IS executives.

In the effort to combat downtime and data loss, there is one protection, detection, and correction tool IS executives should be aware of: professional data recovery services. In many cases, data recovery is not just the most practical and economically feasible method for data protection and retrieval, it is the only method available. Moreover, data recovery professionals can successfully augment the current protection, detection, and correction techniques employed by any organization. The goal of this paper has been to help IS executives better understand data recovery and the many other protection, detection, and correction alternatives available. It is with this knowledge that IS executives can implement better data security and integrity procedures.

If you wish to learn more about data recovery and its place in the protection, detection, and correction model, please visit the ONTRACK web site at <http://www.ontrack.com>. The web site features an in-depth newsletter covering topics related to data protection and recovery, an expansive technical support area, detailed descriptions of the many ONTRACK software and service products, and many opportunities for you to order free literature and educational information. In addition, you may contact ONTRACK at **1-800-872-2599** with any questions or to have information sent to you.

Final Analysis

Additional Information

Selected Bibliography

- “The Audit Commission Report, 1994.” Infosecurity News March/April 1995.
- Bridgeman, Carleen. “Foolproof Solution for the Foolhardy.” Disaster Recovery Journal April/May/June 1994.
- “Bringing Infosecurity Into the Light.” Infosecurity News Jan./Feb. 1995.
- Data Protection Guide. Ontrack Data Recovery, Inc. 1995-1996.
- Data Recovery Lab Report. Ontrack Data Recovery, Inc. 1996.
- “Disaster Recovery: Providing a Safety Net.” Communications Week 28 Aug. 1995.
- “Down But Not Out.” HP Professional Sept. 1994.
- “Financial Impact of Downtime.” Sunexpert July 1996.
- “How Vulnerable is Your Network?” Communications Week 4 March 1996.
- “IS Manager Concerns.” Sunexpert July 1996.
- “LAN Overboard.” Reseller Management Nov. 1995.
- NCSA’s Annual Worry Report.
- “Network Q&A.” PC World Feb. 1991.
- RAID White Paper. IDC.
- Schreider, Tari. “The Legal Issues of Disaster Recovery Planning.” Disaster Recovery Journal 1996.
- Toigo, Jon. Disaster Recovery Planning: Managing Risk & Catastrophe in Information Systems.
- “Vulnerability of Mission-Critical Data Appears to be on the Rise: Special Supplement: Client Server Computing.” Computing Canada 1 March 1995.
- “Wolf in Sheep’s Clothing.” Infosecurity News Jan./Feb. 1995.