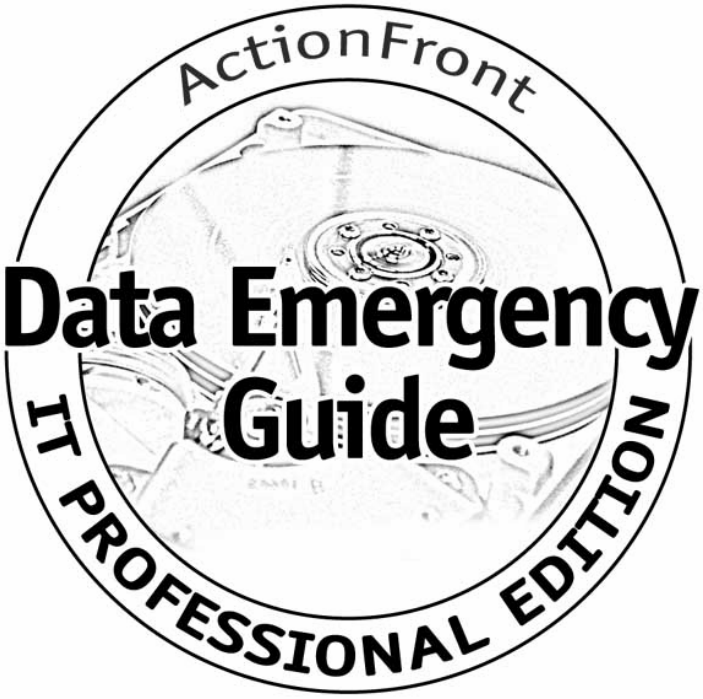


"for IT professionals, data center managers, systems administrators, CIOs, department and workgroup managers, DBAs, small/medium business owners, frontline IT and computer support personnel who maintain mission critical data storage."

Table of Contents

TABLE OF CONTENTS - CONTINUED

Introduction

This guide is intended to help you recognize, react appropriately to and resolve a data loss emergency involving servers, backups, and or any mission critical computer system or IT facility.

The *Data Emergency Guide: IT Professional Edition* will be most useful to technical support personnel, IT managers and anyone experiencing a sudden data loss situation involving a previously functioning computer system or backup, or dealing with the accidental erasure of data or overwriting of data control structures.

For more general information about data storage, backups and data loss prevention for personal computer users, please see the original *Data Emergency Guide*. (Available as a free download at www.ActionFront.com.)

Data Emergency Examples

- A multi-drive RAID server has crashed and no longer serves data to the corporate network. (NAS, DAS or SAN architectures.)
- A set of medical images stored on a digital tape cartridge can no longer be restored to other media.
- Failed upgrade of hardware, O/S or application software.
- Failed restore: an attempt to recover lost data has not only failed but rendered the entire system unusable.

A data emergency usually begins with one of the following situations:

- The sudden inability to access any data from a previously functioning computer system or backup.
- The accidental erasing of data or overwriting of data control structures.

- Data corruption or inaccessibility due to physical media damage or operating system problems.

The situation cannot be resolved "in-house" or with the assistance of vendor technical support or the regular 3rd party maintenance service provider.

Server Data Loss Scenarios

Properly maintained data storage systems are generally reliable, fault-tolerant, and well managed by experienced operators who carry out their routine duties well. When these systems do fail, it is a rare event; often the first time the operator has been faced with these circumstances. It can be (understandably) beyond the training and experience of most of the technical community, let alone the owner/operator or department manager who must double as the systems administrator. Both managers and technicians, especially those who carry multiple responsibilities, can make mistakes when in unfamiliar territory. Our professional data recovery specialists deal with these situations every day and are well qualified to address the problems.

Proper diagnosis of problems is the key to successful management of a data loss emergency. Who is qualified to diagnose your situation? Did you install the system and do you possess the knowledge and experience to diagnose the problem? If someone else set up the system, is it better to call them or other outside experts? A proper diagnosis will then dictate whether:

- To call in our data recovery specialists or
- Initiate a self-fix, (assuming that there is an adequate backup).

If you experience a data emergency in the future, you may well recognize your situation as similar to one of the following scenarios. Proper diagnosis and follow up can save your data and perhaps much more.

Situation 1: Single Failed Drive in a RAID5 Server

- A single drive failure in a RAID5 server has been detected but the server is still operating and serving data to the users.
- The server may or may not have other problems beyond a single failed drive. The operator is not able to do a complete diagnosis.
- Relying on the "hot fix" capabilities thought to be inherent in the system, the operator is tempted to replace the failed drive "on-the-fly" thereby sparing the users any downtime.
- Yielding to the temptation, the hot fix is attempted.
    - If successful, the operator is an unrecognized hero, as the users were never affected by problem.
    - If unsuccessful, the operator may become the very "visible villain" rather than an "invisible hero" and be seen to be responsible for a

prolonged period of server downtime and all the related problems caused by the downtime.

- What should be done in this case:
    1. The very first thing in the proper course of action is to establish the viability of a complete and integral backup of the current data, even if this involves inconveniencing the users. A complete backup at this point is ideal although an incremental backup may suffice if you have a proven restore procedure based on a series of complete plus incremental backups.
    2. Next, restore the backup to the alternate, “contingency” server and prove that it is operational, in case it is needed.
    3. Confident that the contingency infrastructure is ready to go if needed, the operator can proceed with a hot fix attempt or other procedures to address to the situation.

Situation 2: RAID5 Server has Failed

- Multiple drives or a controller has failed in a RAID5 server, causing the server to be inaccessible.
- There is no alternate server available or no adequate backup available to be loaded on the alternate server.
- This means that you are faced with a full-fledged data emergency.
- Many operators faced with this situation will attempt a quick fix by trying some combination of replacing the failed components and reconfiguring the system to rebuild the failed array. Under these conditions, there are two possible outcomes:

  - A functioning server missing much or all of their data. The data and file structures are likely mostly overwritten at this point making a recovery very difficult or impossible.
  - A non-functioning server and dimmer prospects for recovery. The data and file structures are likely mostly overwritten at this point making a recovery very difficult or impossible.
- The appropriate thing to do when faced with these conditions is to call professional data recovery specialists.
- A professional data recovery specialist will begin their process by making a mirror image of the data on each discrete media involved including any failed drives that may need highly specialized data recovery techniques performed in a lab facility. Then working from copies, and using proprietary programs and methods they will rebuild the data set to the point where it can be transferred to a working server.

Situation 3: Server Upgrade Gone Wrong

- Installing new application software, a new operating system or additional or new hardware is often referred to as a server upgrade.
- This is not an everyday event and the operator may lack experience with the process, not understanding, for example, that many upgrades require a data re-initialization process that by nature destroys the existing data or file system.
- During these upgrades a “dialogue box” poses a series of questions the operator may answer without fully realizing the potential impact of the steps involved. For example, the operator starts the data re-initialization process after a warning is misunderstood or ignored. These and other problems can occur during the upgrade that renders the server inaccessible.
- Need to upgrade your server?
  - Never initiate an upgrade without first making sure you have a complete and usable backup. The best way to do this is to restore your backup to an alternate server proving that you have a fully functional redundant server populated with current data.

Situation 4: Intermittent Component Failure in a RAID5 Server

- The electrical and mechanical problems that affect media and its electronic components can be intermittent. While this can complicate any diagnosis, it may also provide an opportunity to obtain a good backup during an interval when the server is functioning correctly.
- Operators may do a “false fix” by replacing a functional component rather than a failed component after misinterpreting warnings generated by the server.

- Some servers have been configured to self-initiate a rebuild under certain circumstances, potentially overwriting otherwise valid media.
- Before addressing an intermittent failure situation we again caution you to:
    - Make sure you have a good backup.
    - Check and double-check your diagnosis.

Situation 5: SQL, Oracle, DB2 Database Corruption

- A server has crashed or experienced O/S problems,
- Tables have been dropped or corruption has been introduced into the actual database.
- The DBA (Database Administrator) has a high level of expertise regarding databases and knows some database specific recovery techniques, but may lack detailed knowledge of data storage platforms.
- They may try to re-initialize the database making the application functional but losing all their data in the process.
- Another attempted fix is to use the transaction logs to “roll back” the database to a “known good state”.
- This can be a good way to solve the problem if:
    - The transaction logs have been examined and deemed to be good.
    - The operation is attempted on an alternate server using a copy of the problem data.
- There is often a preference to try the roll back on the primary server to save time, as restoring to an alternate server can be a very lengthy process.
- If the corruption is a result of physical drive problems that have not been addressed then a roll back on the problem server will only compound the problem resulting in a further degraded system and a more costly data recovery operation.

Situation 6: "Crisis in Progress"

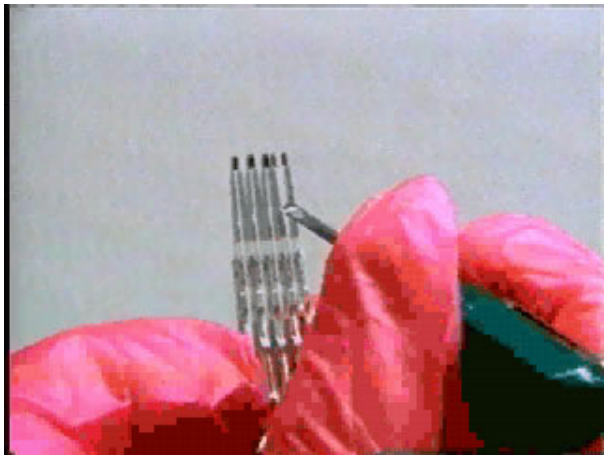
ActionFront is often contacted by an organization that is in the midst of a crisis. The situations have some or all of these characteristics:

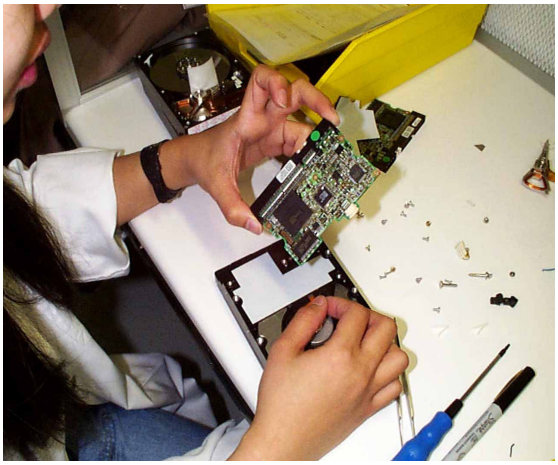
- The server has lost data or become inaccessible to the users.
- Documentation is out of date, sketchy, wrong or simply does not exist and the user knowledge level and understanding of the system is low.
- Backups are available but the process of restoring them is misunderstood or worse, the backups are out of date or do not exist.
- The department manager or the in-house technical teams have tried some fixes.
- 3rd party technicians (from the maintenance service provider or from the vendor) have been called in and tried to rectify the situation and have performed additional operations and attempted fixes.
- The various attempted fixes typically involve swapping out suspect components and/or restoring backups to the original (corrupted) media.
- The server has not been fixed and is possibly further degraded than when the situation started.

While the details may differ, all of these situations have in common:

- Lack of adequate backup and/or no proven restore procedure
- Lack of documentation or knowledge of the system configuration and all the various hardware, software and O/S layers and how they work together.

Professional data recovery specialists will begin any recovery by mirroring each discrete media involved. Knowing that they can always revert to the same starting point, the lack of documentation can then be safely overcome through analysis and experimentation based on strong knowledge and experience of data storage.





Recognizing a Data Loss Situation

A data loss situation is usually characterized by the sudden inability to access data involving a previously functioning computer system or backup or the accidental erasure of data or overwriting of data control structures. This section outlines the major symptoms of data loss.

Server Data Loss Symptoms/Issues

- Symptoms Related to Physical Problems
  - Sudden Server crash during operation or power up.
  - Ticking or grinding noises coming from one of the hard drives while powering up or trying to access files. This symptom may precede actual data access problems as the drive utilizes spare sectors.
  - Single hard drive failure.
  - Multiple drive failure.
  - RAID controller alarm flashing..
  - RAID controller failure rendering drives inaccessible.
  - Intermittent drive failure resulting in configuration corruption.
  - Visible fire or water damage.
- Symptoms Related to Soft (Logical) Problems
  - Server will not reboot after “routine” upgrade to operating system or applications.
  - Boot drive filesystem problems involving the loss of critical configuration data.
  - Server storage systems registry configuration lost/overwritten.
  - Accidental deletion of data.
  - Accidental reformatting of partitions.
  - Accidental reconfiguration of RAID drives.
  - Accidental replacement of hard drive.
- Soft (Logical) or Physically Related Symptoms (Could be either)
  - Server reboots but cannot access or even “see” attached storage.
  - Failed or prematurely aborted restore.
  - Applications are unable to run or load data.
  - Extreme degradation of application performance.
  - Folders that should be full of files open but appear empty.
  - Inaccessible drives and partitions.
  - Corrupted data.

Tape Media Data Loss Symptoms/Issues

- Corrupted tape headers:
  - Tape appears empty of data (blank) but should be full.
  - Tape should be full but has very little data.
  - The tape is invisible to or inaccessible to the restore program.

- Accidental reformatting or erasure of tape.
- Tape has become un-spooled inside the cartridge.
- Obvious physical damage.
    - Tape media stretched, snapped or split.
    - Visible fire or water damage.
- Media surface contamination and damage.
    - Tape cannot be read past a worn-out or contaminated area.
- Tape backup-software problems involving corrupt catalogue information or corrupt data control structures.

Optical Media

- Sector read errors preventing access.
- Corrupted filesystem structures show empty or invalid (e.g. FAT, directories, partition entries).

Auto-loaders and Jukeboxes

Both optical and tape media libraries or multi-volumes can be maintained through automation. To secure an archival copy, a backup copy to be kept offsite or for other reasons, rotations are required by the technicians to cycle the media in and out of the autoloaders. As these can be complex systems, any rotational error can cause data to be over-written.

Tape media can occasionally suffer physical damage due to tape drive mechanical problems. The damage can be increased by automation, as a robot trying to remove such a tape from a drive will not recognize the problem whereas a human operator has a better chance of removing the tape without causing further damage.

Corrupted/Damaged Databases

- The database is marked as “suspect”, preventing access and it cannot be restored to a functional state.
- Tables have been “dropped” or recreated.
- Backup files not recognizable by database engine.
- Accidentally overwritten database files.
- Accidentally deleted records.
- Corrupted database files or records.
- Damaged individual data pages.

Experiencing a data emergency? The most important question to ask yourself or your users is:

"How important is your data?"

The answer to this question will help you choose an appropriate course of action.

1. **My data is Very important:** To most people experiencing a data loss emergency, restoration of application data is of equal importance as making the system operational again, i.e. the system and the data together define an "operational system". If data is important then follow the first principle of data recovery to: **"DO NO HARM"** as you address your situation and remember that you can call on specialized Data Recovery help.

2. **My data is Not important:** In some circumstances, the priority will be to get the systems operational again regardless of the status of the application data. If this is the case, you are not experiencing a true data emergency. You can likely treat the situation as a brand new install and make use of the same human and IT resources that initially set up and configured the installation.

Damaged Media (DLT Tape)

Data Recovery Process: What to do first?

What NOT to do:

If you are facing a data loss situation, what NOT to do is very important!

- Never run a program or utility that writes to or alters the problem media in any way. If the system shows symptoms of a physically damaged device or symptoms of data corruption:
  - Never restore a backup.
  - Never reinstall software or O/S.
  - Do not reinitialize the media or database.
  - Do not attempt to roll back the database to a known good state.
- Do not allow anyone else to write to or alter problem media including companies that offer "Remote Recovery Services". If for some reason your restore goes awry, you may have created a situation where a potential recovery from the original media may no longer be a viable option.
- Do not power up a device that has obvious physical damage.
- Do not power up a device that has shown symptoms of physical failure. For example, drives that make 'obvious mechanical fault noises' such as ticking or grinding, should not be repeatedly powered on and tested as it just makes them worse.
- Activate the write-protect switch or tab on any removable media such as tape cartridges and floppies. (Many good backups are overwritten during a crisis.)
- Do not attempt to remove a damaged or unspoiled tape from a drive unless you have the specialized knowledge and equipment to do so.

What to do:

Review, Record and Remain Calm

When facing data loss, stop and review the situation. Distress and even panic are typical reactions under the circumstances, so the process of reviewing and writing down a synopsis of the situation has the dual purpose of preparing for a recovery and inducing calm.

Resist the Pressure for an Instant Fix

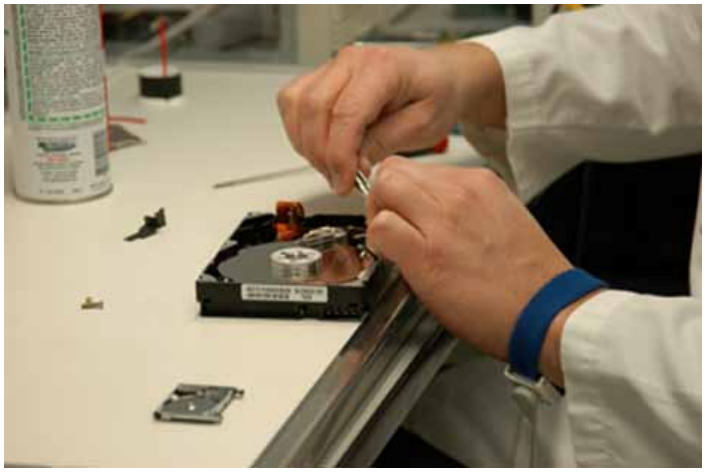
If you have "recognized a data loss situation", stop and analyze the situation rather than attempt to fix it immediately. You may be under considerable pressure from co-workers, your boss or even your own deadlines to immediately resolve the situation. While a quick fix may prove successful, if it is not, then your attempts may actually increase the damage and greatly reduce the prospects of a successful data recovery.

Beware DIY Solutions and Products and Remote Recovery Services
There are numerous Internet sites offering advice about data recovery and vendors offering DIY (Do-It-Yourself) software solutions. Unfortunately the advice is often just plain wrong and DIY software or remote recovery services may complicate your problems and diminish the prospects of a successful recovery should these software recovery attempts fail. Note also that there is no software in the world that can fix storage media with physical defects.

Set up an Alternate System
Consult your company's systems documentation to configure another computer/server to temporarily replace the problem unit. Restore whatever backups are available onto this unit and reconfigure it as necessary to begin productive work. Of course, the more time that has been spent on contingency planning before the data loss, the less time it will take now to set up an alternate system.

Disk Drive Handling and ESD (Electrostatic Discharge) Precautions
Before handling your computer and especially before touching or handling the media itself, beware of creating static electrical discharges. (See appendix C.)

Call ActionFront Data Recovery Labs (800) 563-1167
Our data recovery consultants will answer all your questions and help you determine how to address your situation. If data loss is confirmed, you will receive advice about how to send in your media, a promise on turn-around time for the free evaluation, what to expect regarding price range and what factors may affect how fast we can recover your data.



Data Emergency Worksheet

The following pages are designed as a workbook to help you prepare for a successful recovery from your data emergency.

1) When was the system last running fine?

2a) What happened since then: regarding operator activities?
2b) What happened since then: regarding any symptoms of problems?

3) Are there any specific error messages?

4a) Backups History: The last “complete backup” of the entire system.
4b) Backups History: Dates and details of “incremental backups”.
4c) Backups History: Dates and details of partial backups (ex: selected data files).

5) Specific databases and directories that are important to you?

6) List the details of your configuration such as:
6a) Operating system name and version (Windows NT, Novell, Unix version, etc)
6b) System set up, partitions and storage configuration?

6c) Application software packages installed?		
Names	Versions	Original CDs and Documentation Avail.?

6d) What login passwords are required?

7a) Do you have a contingency plan?
7b) What are your resources at hand to implement it?
7c) Can you run your applications on a “spare” server?
7d) Can you attempt to restore the backup you have to the spare server and leave the problem unit alone for now?

8) Are you or your technicians qualified to make a proper diagnosis?

With a complete set of notes, and perhaps an interim solution in place, you are now ready to call a data recovery professional at 1-800-563-1167 or through email, helpme@actionfront.com or visit www.actionfront.com.

ActionFront's Data Recovery Process

Initial Inquiry and Consultation Process

The ActionFront CSR (Customer Service Representative) will follow the medical oath to "do no harm", and will seek to analyze, preserve and stabilize the current situation. Keeping the usually distressed customer calm, they will seek answers to the questions listed above, in order to fully grasp the situation at hand. An ActionFront CSR will be able to confirm that you have a data loss situation that they can help you with.

Once a data loss situation has been confirmed, you will either ship the problem media to the nearest ActionFront Lab or arrange for on-site (Critical Response) service if required.

If possible, we recommend removing the media from the computer before shipping. Beware of creating electrostatic discharge (ESD – see Appendix C) while handling your media. Visit the ActionFront website (www.actionfront.com) for more information about packaging.

The Recovery Process Begins with a Free Evaluation

After carefully inspecting the problem media and reviewing all the information available about the case, the ActionFront technicians provide a full diagnostic report to the CSR, who then provide the customer with a definitive quote. The diagnostic is performed and the quote provided at no cost to the customer.

Fixing Physical Problems

Approximately 70% of cases have some sign of physical failure. If this is severe, some (temporary) hardware fixes may be necessary before even the diagnosis can be completed. These would include:

- A “board swap” whereby a defective PCB (printed circuit board) on the drive is exchanged for a working board.
- A “head transplant” whereby a defective read/write head on the drive is exchanged for a working head.
- A “platter or motor transplant” for certain models.

Obtaining a Mirror Image (Making a Copy of the Data)

As the problem media may completely fail under repeated use, a “mirroring” process (i.e. making a special copy of the data from the problem media) is the first priority during the diagnostic phase. In most cases all subsequent recovery activities take place on the mirrored copy.

Fixing Logical Problems: Corrupted Files or File Systems

The next step is logical retrieval of data. Working with the mirrored copy of the data and using proprietary software programs, our programmers fix corrupted files systems and put corrupted files back together, with a focus on the customer’s priorities.

Tracking the Case

Our web-based, online, proprietary “JobTrack” system forms the “central nervous system” of the ActionFront process. JobTrack records and publishes timeline and other commitments to our customers because keeping promises is integral to the ActionFront business model.

Customers use their case number and a private password to gain access to the JobTrack system via the ActionFront website and can self-track the step-by-step process involving their media’s recovery and review related quotes and invoices.

Our staff members also use JobTrack to document and manage our workflow process. It is maintained by ActionFront staff across all our locations and is a primary tool to enforce ISO 9001:2000 compliance and provide extraordinary customer service levels. It is an integrated system serving all departments in all locations, while maximizing the efficient use of resources.

Costs vs. Value

- ActionFront can determine the **cost of a recovery**. ActionFront's rates for data recovery are based on a number of factors:
    - Complexity of the problem.
    - Amount of labor involved.
    - Amount of lab time and other resources required.
    - Availability (or scarcity) of parts.
- Only the "owner" of the data really knows the ***value of the data***.
- ActionFront provides a firm quote detailing the expected timeframe and outcome of the recovery. With this in hand the customer can decide:
    - If the value of the data is greater than the cost of the recovery.
    - If the cost of the recovery is more than the cost of manually inputting/recreating the data.
- ActionFront customers have final approval on whether or not the recovery was successful.

ActionFront provides two distinct service levels: Priority and Critical Response.

Priority Service Features

- This in-lab service level meets the urgency requirements and fits the budget resources for most ActionFront customers.
- Free evaluation.
- Fast turn-around of evaluations and recoveries.
- No files = no charge.
- Data guarantee. Our money back guarantee assures the return of usable data.

Priority Service Step-by-Step Workflow

- Priority service means that ActionFront CSRs and lab personnel devote an extraordinary focus to each job that begins with the first phone call from the (usually) distressed customer.
- Upon receipt of the customers' media, the ActionFront CSR immediately informs the customer of their case number and password, and that their job has arrived and that we have already begun our evaluation process.
- The method of communication, based on customer preference can take place via phone, email, fax and of course our web-based online "JobTrack" system available on a 24/7 basis.
- Initial evaluation results are communicated as soon as they are available, often within a few hours of receipt.
- All customers are contacted about their job status within 10 business hours.

- Our customer service process involves intense communication between the lab, the CSR and the customer and is based on years of successfully retrieving lost data.
- After the customer has approved the quote, the lab proceeds to the next stage and produces a list of the files that can be found, the condition of the files and any other pertinent information. The CSR then confirms with the customer that we have indeed found the data they need and are willing to pay for. With this confirmation in hand we proceed with the final stages of the recovery.
- We present a summary of the outcome to the customer, and then secure payment prior to shipping the data back to the customer on the return media of their choice.
- Whether the Priority Service can be completed within one day, a few days or more depends on the availability of the customer for the Q&A process and the complexity of the recovery job.
- CSRs are available six days per week Monday-Friday from 8 a.m. through 7 p.m., and Saturday 9 a.m. through 5 p.m. (EST). Website and voice mail support is available 24/7 and customers with extremely urgent needs can use these to access our emergency Critical Response Service that operates on a 24/7 basis.
- Keeping promises is fundamental to the entire process.

Pricing for Priority Service
All priority cases receive a free evaluation, and a Data Guarantee. If there is no data recovered there is no fee.

Single-hard-drive recoveries:
- $500 (Minimum charge)
- $1,200 (Average charge)
- $5,000 (Exceptional cases)

Removable Media (Photo Cards, Zip, Optical)
- $250-$500

Complex Recoveries (Multi-drive servers and backups)
- $2,500 to $10,000 (Typical cases)
- Greater than $10,000 (Exceptional cases)

Critical Response Service

The Critical Response Service is available 24 hours a day, 7 days a week. The ActionFront Critical Response Team is comprised of the best of the best data recovery technicians who take turns being on standby, ready to travel anywhere at a moments notice.

The team is called for all kinds of mission critical recoveries including combinations of network servers, RAID, NAS, SAN, tape autoloaders and optical jukeboxes, and corrupted file sets in software platforms such as SQL, Oracle and Exchange Server.

On-site service is available for emergency situations where immediate shipping to one of our labs is not feasible or security procedures prevent the media from leaving the data center.

Whether the case is handled in the lab or on-site, we work around the clock to restore mission critical operations. Our first step is always to analyze then stabilize the situation before we attempt the recovery.

Unlike the free evaluation provided under our Priority Service, there is a non-refundable fee of $5,000 to engage the ActionFront Critical Response Team. Pricing for the entire project will then be negotiated during the initial engagement phase.

Appendix A: What is Data Recovery?

It may not be what you think it is!
Many people equate data recovery with restoring data from a tape backup, or use the term “data recovery” interchangeably with “disaster recovery” as in recovering from a major disaster such as a flood, fire or bombing attack. These meanings are quite true in the general sense and “data recovery” is usually one step of the “disaster recovery process.

However, the term “Data Recovery” has a very specific meaning in the computer industry. First, consider one of the dictionary’s definitions for ‘recovery’.

‘Recovery’ *noun*.
“The act of obtaining usable substances from unusable sources.”

Based on this, ActionFront offers the following definition.

‘Data Recovery’ *noun*.
“The act of obtaining usable data from downed computers and backups and corrupted file sets.”

Data recovery cases can be divided into two broad categories:
Common Recoveries
Involve floppies and hard drives that are usually from single-user personal computers.

Complex Recoveries
Involve hard drives, RAID arrays, tape and optical media or corrupted databases and file systems usually from multi-user, business systems. Data storage at the high-end has become a very complex field. In the case of these complex situations data recovery can be seen as “troubleshooting data storage”.

Whether common or complex, each data recovery case is unique and the process can be very resource intensive and exceedingly technical.

Appendix B: Case Studies of Mission Critical Recoveries

460GB RAID5 Crash at California Technology Company

- RAID upgrade from 6 drives to 8 appeared successful.

- Subsequent reboot precipitated loss of all access to the data stored on the RAID5 server.
- Server urgently needed for a product launch.
- Friday evening crash; ActionFront's *Critical Response Team* had the recovery underway within 3 hours.
- On-site and remote technicians worked around the clock.
- Complete turnaround in 36 hours! Product launch was successful supported by the fully functional 8-drive server.

Database Corruption

- An Internet based financial services company maintained all transaction records in a large SQL database on their corporate server.
- A routine software maintenance program was run periodically without problems until the operator made an error while launching the program.
- A number of the database tables were "dropped", then recreated and re-populated with data thereby over-writing some of the data and damaging the file structures causing the main application to crash.
- A recent backup was not available.
- Without this mission critical data and associated application, this business was doomed to face imminent extinction.
- ActionFront analyzed the server and a majority of the missing data was identified as recoverable. No physical problems were found, confirming this case as a complex logical recovery.
- The customer identified the most critical of the missing tables and in order to contain costs, ActionFront was directed to focus their efforts on these tables.
- The critical tables were recovered and returned to the customer who was soon back in business.

Lost Diagnostic Images on DLT Cartridges

- Large urban hospital in the US North East was generating approximately 90,000 medical images per day requiring about 25GB of digital data storage.
- They have a regulatory requirement and an obligation to patients to provide the original images.
- Tape rotation errors caused erroneous EOD (End-of-Data) markers.
- IT vendor stumped or lacking resources to resolve the problem.
- Proprietary expertise required.
- Time intensive recovery due to the nature of tape problems.
- The hospital regained access to the lost images and was able to provide the high standard of health care their staff and patients demanded.

Appendix C: Handling Tips & ESD Precautions

Mishandling is a leading cause of hard disk drive failure.

Hard Disk Drive Do's

- Handle a hard disk drive as you would handle an egg.
- Always use ESD* precautions.
- Handle drives one at a time.
- Handle drives only by the sides.
- Pad all hard disk drive work surfaces.
- Handle failed hard disk drives with the same care as new drives.
- Wait 10 seconds after power down before moving to assure the drive has stopped spinning.
- Eliminate movement of unprotected drives: Use ESD packaging (anti-static bag) while moving and minimize the number of handling steps.

Hard Disk Drive Don'ts

- Never drop drives.
- Never allow drives to come in contact with hard surfaces.
- Never stack drives, even in the ESD protective bag.
- Never contact the PCBA with tools or without ESD protection.
- Never stand drives on end.

Disk Drive Components Susceptible to Handling Damage

- Heads - Broken, chipped, degraded.
- Disks - Scratched media, head slaps.
- PCB - ESD damage, bent connector pins, broken components.

***ESD (Electrostatic Discharge)**

A familiar form of Electrostatic Discharge, often called "static electricity", is the shock we receive after walking across a carpet. In a technical environment, ESD can be very costly by harming devices or components. ESD may cause a catastrophic failure that appears immediately or a latent failure in which gradual degradation occurs during use, resulting in eventual failure.

ESD Precautions

- Computer professionals should purchase ESD wrist straps, floor mats and educate themselves on the ESD precautions.
- A personal user should discharge the static on themselves by touching a metal object before touching a computer, hard drive or other component.
- People in very cold or dry areas should be aware that humid air helps to dissipate electrostatic charges.

Our Pitch

Customers with a Data Emergency Need

- Urgent Service and Intense Communication.
- Ability to control process.
- Pricing Integrity.
- Usable data returned to them ASAP.

ActionFront Delivers

- Fast turnaround for in-lab evaluations and in-lab recoveries.
- Free evaluations.
- No files = no charge.
- Data Guarantee.
- CSRs use phone, email, fax, JobTrack or whatever means necessary to keep the customer informed of the status of their case, to make sure we are focused on the customer's priorities and to seek on-going approval to continue the recovery process on their behalf.
- Tools and processes to keep the customer in control of the process.
- Customer satisfaction, usable data.

ActionFront Strengths

- ISO 9001:2000 Certification.
- Manufacturers support. We are permitted to open virtually any hard drive without voiding the warranty and enjoy referrals from many manufacturers including Maxtor, IBM, Quantum, Western Digital, Seagate, and Dell.
- All hard disk drives & floppies.
- O/S: all versions of Windows, Mac, Unix.
- Complex Recoveries:
    - Servers: RAID, NAS, and SAN.
    - Magnetic tape & optical storage.
    - Autoloaders, Libraries, Jukeboxes.
    - File "repair": SQL, Oracle, Exchange Server.
- Recovery team: CSR + Lab + the Customer!
- Urgent attention to each case.
- Old, new and complex technology.
- Un-matched expertise gained across a wide variety of hardware/software combinations and data loss situations.
- Extensive investments in the latest technology, continuous improvement in methodologies and skilled people.
- Experience serving the most demanding customers.
- Usable Data returned to customer.

Next Steps

Backup, restore and maintain your systems.

Visit and bookmark: www.actionfront.com.

Spread the word on Data Recovery.

Data Emergency?

When in doubt, check with a professional data recovery expert at:

1 (800) 563-1167

helpme@actionfront.com

Our success is based on
providing free evaluations, fast turn-around times and
solutions that guarantee the return of usable data.

Atlanta, Buffalo, Chicago, Santa Clara, Toronto and Tokyo