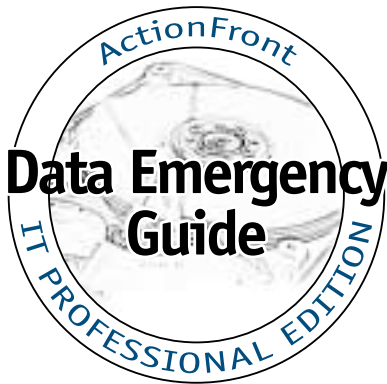# DATA EMERGENCY GUIDE

ACTION FRONT
DATA RECOVERY LABS

Attention IT PROFESSIONALS

For additional information on complex data loss situations with a specific focus on server problems visit www.ActionFront.com today, and download the new

ActionFront

Data Emergency Guide

IT PROFESSIONAL EDITION

Partial Table of Contents:

Server Data Loss Scenarios

Situation 1: Single Failed Drive in a RAID5 Server
Situation 2: RAID5 Server has Failed
Situation 3: Server Upgrade Gone Wrong
Situation 4: Intermittent Component Failure in a RAID 5 Server
Situation 5: Oracle, DB2 Database Corruption
Situation 6: Crisis in Progress

Table of Contents

Copyright 2002, 2003

Introduction

This guide is intended to help you recognize, react appropriately to and resolve a data emergency.

It is not a technical support manual for the installation, configuration and upgrading of data storage devices and platforms, nor is it a how-to manual for data backup procedures.

The Data Emergency Guide will be most useful to computer users and technical support personnel 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 general technical support and/or consultation on proper backup systems please consult your data storage vendor or your local computer systems supplier/integrator.

This guide does include some excellent reference materials about data storage, backups and data loss prevention, with links to additional reference materials and links to vendor technical support.

The Importance of Data Storage

Data Storage is the holding of information in a digital format on a device or system of devices that are within or attached to a computer system. Examples of data storage devices range from those found on personal computers such as a hard drive, a floppy diskette, or a CD-ROM to those found in sophisticated corporate data centers such as large multi-hard drive servers and automated backup libraries. Data storage is an integral component of all computer systems and modern life, as we know it, would not exist without it.

The types of information stored can range from simple one-page documents belonging to an individual, up to and including huge commercial databases consisting of millions of records serving thousands of users.

There can be cost savings when replacing paper records with digital records, however the key benefits of digital data storage are the efficient change, replication and sharing of the stored information. For example, a personal user can update and send a resume in minutes to respond to different opportunities. A geographically disparate product supply chain involving multiple companies can collaborate effectively on a just-in-time inventory requirement.

Of course a business can become totally dependant on the application that uses the data storage in their computer system. Losing access to that data can have costly and even catastrophic consequences. A personal user can lose work that took days, weeks or longer to produce if they experience data loss. Sometimes the data cannot even be re-created.

Data storage systems can be large, sophisticated installations of almost overwhelming complexity. Despite redundancy and backup, they can be fragile and unreliable due to human error, adverse environmental conditions and occasional device failure. Even the smartest and most experienced technicians working with the best data storage equipment experience data loss.

What is Data Loss?

A data loss situation is usually characterized by one (or more) of the following:
• 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.

Data loss can be caused by physical damage or "soft" (logical) problems. For example:
• A personal user can no longer access the "C:" drive on their PC or no longer read a floppy disk.
• A corporate data server has crashed and no longer serves data to the corporate network.
• A set of medical images backed up on a digital tape cartridge can no longer be restored.

Have you experienced data loss?
If your answer is "yes", then you are not alone! The majority of computer users will encounter this situation at some time.

Physical Causes of Data Loss

Approximately 70% of data loss cases processed by ActionFront were caused by physical problems.

Occasionally manufacturing defects or design flaws can cause mechanical or electronic failures. Most physical problems can be traced to other root causes.

Physical problems include mechanical failures due to:

• Shock from device being bumped, dropped or moved while operating causing a head crash or platter misalignment.

• Device exposed to extreme cold temperatures and/or rapid temperature change prior to use. For example powering up a laptop after being in a freezing car overnight.

• Disasters such as flood, fire (including sprinkler-water secondary damage) and explosion.

• Stiction: The read-write head assembly gets "stuck" on the disk media due to deterioration of the lubricant or because it has failed to retract to its rest (parked) position.

Physical problems also include failure of electronic components on the drive's controller board due to:

• Electrostatic Discharge (ESD) or heat.

• Power loss or power surge.

Physical problems affecting the computer equipment may also render data inaccessible even though the media (that it is stored on) still functions perfectly:

• Sudden power loss may corrupt open database files.

• Computer memory glitches may result in bad data being written to sensitive filesystem control areas.

"Soft" Causes of Data Loss

"Soft" causes in this context means non-physical causes. These are also referred to as "logical" causes. Soft problems can usually be related back to something that someone did or did not do, in other words "human error". Oops!

• Accidentally deleting files or reformatting the system.

• A tape containing a good backup was partially overwritten because it was inserted out of sequence during a tape rotation.

• "Failed restore". Restoring from a backup can be a lengthy and error prone process. This can include tape format or compression errors.

• Viruses. The malicious work of a smart sociopath.

• Configuration errors due to the complexity of the system.

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 or deleted file-sets."

Data recovery cases can be divided into two broad categories:

Common Recoveries
Involve single hard drives from a PC, MAC or Notebook or removable media such as a photo card or zip disk.

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.

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. What to do and what NOT to do when experiencing data loss is covered under the heading "Data Recovery Process: What to do first?"

Common Data Loss Situations

Single hard drives from A PC, MAC or Notebook
General Symptoms of Computer Problems:
- Intermittent freeze-ups, keyboard or mouse malfunctions, blank or flickering displays or an inability to access networked resources may be symptoms of computer problems that are not data loss situations. A call to your local technical support person at a computer store or corporate help desk is recommended as long as they do nothing during their troubleshooting that will risk hurting your data.
- A simple problem that can stump beginners or casual users is "no power up". Check to see if the PC is plugged in and the wall socket is working or if the internal power supply inside the computer has failed.

Typical Symptoms/Characteristics of a Common Data Loss Situation
- Accidental deletion of data.
- Accidental reformatting of partitions.
- Hard disk crash or hard disk component failure.
- Ticking or grinding noises coming from the system unit where the hard drive is located while powering up or trying to access files. This symptom almost always indicates a failing hard drive and is often accompanied by some of the other symptoms.
  Note: Most drives will emit a light mechanical hum that a user may notice under normal operation. An indication of impending failure is when the "normal sound" changes to louder ticking or grinding noises. This symptom may precede actual data access problems as the drive utilizes spare sectors.
- Computer won't boot. Blue or black screen after power up. The system will not load Windows (or other O/S).
- Applications that are unable to run or load data:
  – Trying and failing to start an application such as Excel or Word.
  – Trying and failing to load a file while running Excel or Word.

- Opening folders that should be full of files but appear empty.
- Inaccessible drives and partitions.
- Corrupted data.
- Visible fire or water damage.
- Media surface contamination and damage.

Complex Data Loss Situations

For additional information about complex data loss, download the "IT Professional Edition" of this guide at www.ActionFront.com.

Note that individual media in servers can suffer from all the same issues detailed in the preceding section. Include the above list of symptoms while diagnosing complex data loss situations.

Servers
Including single drive, RAID, NAS and JBOD type servers.
- Server crash during operation or power up.
- Server will not reboot after "routine" upgrade to operating system or applications.
- Server reboots but cannot access or even "see" attached storage.
- Boot drive problems regarding losing critical configuration data.
- RAID controller failure rendering drives inaccessible.
- Hard drive failed.
- Failed restore.
- RAID alarm ignored.
- Server registry configuration lost.
- Intermittent drive failure resulting in configuration corruption.
- Accidental reconfiguration of RAID drives.
- Multiple drive failure.
- Accidental replacement of hard drive.

Tape Media
- Corrupted tape headers:
  - Tape appears empty of data (blank) but should be full.
  - Tape should be full but has very little data with an early EOD (End-of-Data) marker.
  - Accidental overwriting of headers renders the tape invisible 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 corruption.

Optical Media
- Sector read errors preventing access to certain files.
- Message: "This disk is not formatted. Would you like to format now?"
- 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, an (offsite) backup copy 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 or incorrect EOD markers to be written to the tape.

Corrupted/Damaged Databases and File Systems
- The database is locked as "suspect", preventing access and it cannot be restored to a functional state.
- The file header tables have been "dropped", deleted 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.

Data Recovery Process: What to do first?

If you have "recognized a data loss situation", this section will help you prepare for a recovery, avoid some typical mistakes and perhaps help you operate with an interim solution until the problem is resolved. After reading this section and completing the "Data Emergency Worksheet" you will be well prepared to call a data recovery professional. (You can of course, call us immediately, or at any time, for data emergency advice at 1 (800) 563-1167.)

What to do first?

As in the medical profession, the first principle of data recovery is: "**DO NO HARM".**

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.
- 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 problem removable media such as tape cartridges and floppies. (Many good backups are overwritten during a crisis.)

If you are having data access problems and your media has no symptoms of physical failure or damage, try and check some obvious issues before deciding if you need data recovery:
- Read or briefly review this guide to the end.
- Are the power and drive cables properly connected?
- Is configuration or driver information correct?
- Try the defective unit with a different adapter/controller interface or on a different computer.
- Is there an experienced technician at a local store or the company help desk that you can consult, if these steps are beyond your capabilities? (Make sure whoever is in contact with your data loss situation is fully aware that they should do nothing during their troubleshooting that will risk hurting your data.)

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

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 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. See Appendix D for more information about this topic.

Set up an Alternate System

Do not attempt to restore a backup into or onto the original corrupted data set as you may over-write some of the lost data. Furthermore, 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.

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. Obviously, the more time that has been spent on the contingency plan 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. (Often just called "static", this is the electrical spark you experience while touching a person or object, especially in a dry environment.) See Appendix C.

Data Emergency Worksheet

The following pages are designed as a workbook to help you prepare for a successful recovery from your data emergency. You may want to make extra copies before you begin.

Data Emergency Worksheet

- How important are your data files?
- Do you need to preserve your data and be able to restore it along with your system?
- If "yes" then proceed with this worksheet and answer all the questions you can.
- Do not attempt (or allow a local technician to attempt) to restore a backup to a problem drive or server or use any Do-It-Yourself utility that writes to or alters the problem media, as you may permanently lose your data. (See Appendix D.)

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 file names and directories that are important to you? (Or, what applications generated or used these important files?)

   _____
   _____
   _____
   _____

6. Can you remember details of your configuration such as:

6a. Operating system name and version (Windows 98, NT, Novell etc)?

   _____

6b. System set up and partitions, sizes (drive "C: D:" etc)"?

   _____
   _____

6c. Application software packages installed?

Names	Versions	Original CDs and Documentation Avail.?

6d. What passwords are required for:

   Start up?_____
   Access to the hard drive? _____
   Specific directories?_____

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" computer?

_____

7d. Can you attempt to restore the backup you have to the spare unit and leave the problem unit alone for now?

_____

8.   Is there a technician at a local store or the company help desk that you can consult to analyze the problem or help implement the contingency plan?

_____
_____

9.   Is there a technician available to help you remove your problem media and prepare it for shipping?

_____

10. Is there a technician available to assist in the re-install and reconfigure process once you have received your recovered data?

_____

With a complete set of notes, and perhaps an interim solution in place, you are now ready to call a data recovery professional. See Appendix E "How to Choose the Right Data Recovery Company" or call 1 (800) 563-1167.

Initial Inquiry and Consultation Process

A good data recovery consultant (such as the ActionFront CSR or Customer Service Representative) will follow the medical oath "do no harm", and 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 ship the problem media to the nearest ActionFront Lab.

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 http://www.actionfront.com/us_packaging.asp for more information about packaging.

Starting the Recovery

After carefully inspecting the problem media and reviewing all the information available about the case, the ActionFront technicians begin a "mirroring" process if the submitted unit is physically functional, (i.e. they make a special copy of the media in question). In most cases all subsequent recovery activities take place on the mirrored copy. As the media in question may completely fail under repeated use, using this process increases the chances for a complete recovery and preserves the original media in case further access is required.

Next Recovery Steps

Approximately 70% of cases have some sign of physical failure. If this is severe, some hardware fixes may be necessary before even the mirroring can take place. 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.

Logical or software retrieval, working with the mirrored copy, comes next while the technicians focus on the customer's priorities.

A detailed account of the recovery and customer service process at ActionFront follows in the next section.

ActionFront's Data Recovery Process

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.

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.

Customers use their case number and an issued 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.

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

Priority Service
• In-lab service.
• Free evaluation.
• No files = no charge.
• Data guarantee: Our money back guarantee ensures that useable data is returned to the customer.

Priority service means that ActionFront CSRs (Customer Service Representatives) and lab personnel devote an extraordinary focus to each job that begins with the first phone call from the (usually) distressed customer.

*Both **common and complex recoveries** are performed under our Priority Service. In fact, Priority Service meets the needs and time-line expectations of almost all our clients.*

• We track in-bound cases to make sure they arrive on time.
• 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.
- Each case is unique and sometimes requires several cycles of questions and answers (Q&A) before we present the customer with a quote.
- 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 "estimated 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 useable 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
Critical Response Service is for the select few clients that need an extra-ordinary level of around-the-clock service and have sufficient budget resources available.

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.

Our Critical Response Service addresses only the most **complex recoveries**.

The team is called for all kinds of complex 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.

Case Studies: Real Life Data Recovery Stories

Common Recoveries

Client Database Missing from Desktop System
- A consultant used a Sales Contact Database program to manage her customer information and account activities.
- She was suddenly unable to load the application and local technical support reported finding "empty" files.
- ActionFront found and overcame physical problems by opening the drive in clean room conditions.
- The consultant purchased a new drive at cost from ActionFront, which was loaded with a usable version of her completely restored database.
- Here is what the customer said in response to our standard follow-up request for feedback:

"I have to say that I was extremely impressed with ActionFront Data Recovery. The customer service representative took the time to explain and translate my hardware/data situation and was very helpful in offering me options and potential solutions to my data problem.

On the technical side your website was very useful and kept me up to date on the status of my recovery. It was very well presented and your commitment to customer service was apparent.

Losing my data meant losing many of my clients' files and a year+ worth of work on my part. Recovery, though a very large hit to my pocketbook, meant I didn't have to go and explain to my clients that I had lost the data and the work that they were paying me to do!! On a positive note it's a tax write off!! ;)

Thank you ActionFront and good work!"

MS Word files cannot be read on a Floppy Disk
- This case history is copied directly from an email sent to ActionFront.
- This recovery was a technically simple one, and provided "pro bono" under the ActionFront complimentary recovery policy.
- The name of the customer's employer and a few details have been changed for confidentiality reasons, otherwise this is in the customer's own words. (Note: Brent is an ActionFront CSR and Sam is the VP of Customer Service.)

"Here's my feedback. Sam was a lifesaver and Brent was a tremendous help through the beginning stages of this process.

I work for a Rape Crisis Program. We work with survivors of rape, domestic violence, incest and sexual assault. The document I was working on was the Emergency Department (ED) protocol for cases of sexual assault/abuse. I had been working on it for months and yes; I was stupid enough to not save it on my hard drive. The documents were saved on a floppy disc, which I carried everywhere since I was working on it all the time.

I had incorporated feedback from the director of the ED, director of nursing from the ED, different ED staff and my director. (Yes, you can say it, how stupid can I be not to save it somewhere else). Anyway, if I did not receive those documents I would have to confront a lot of people with a lot of embarrassment and would have lost all credibility. Sexual assault is already a crime that is not taken so seriously and my credibility in the institution is crucial. Losing this file would have meant to start all over again and I was not able to sleep for a few days.

I initially spoke to Brent and he calmed me down. He was extremely nice and patient with me (I was about to have a nervous breakdown). He did not promise anything, but said they would try to do everything possible to retrieve the data. Finally, Tuesday night I got the call from Sam and I wished I could fly to Toronto and give him a hug. He then gave me more good news because I would not be charged for the service. I almost wanted to cry. Our program is a non-profit organization and we are funded by private donations and state/federal grants. I would have had to pay for it out of my own pocket and if you didn't know, counselors don't get paid much.

Anyway, I know that you probably deal with much bigger problems and more important information, but I wanted you to know how grateful I am for the service that was provided. I found out about you, through the Internet. I went into google.com and typed "data recovery new york city" and there you were. The reason I chose you was because it said "free evaluations", so I had nothing to loose except the money spent on shipping it to you. I called and spoke to Brent and the rest you have read already.

Thanks again for your wonderful service!!!!!!!!! I will keep your number in a very valuable spot."

Photos on a Damaged Microdrive
- Tiny media damaged in a fall.
- Family event photos of high sentimental value.
- Difficult recovery working with very small components.
- Complete recovery of photos returned on CD.

Julia loved her present, a digital camera with an IBM Microdrive that held loads of photos. She immediately began taking photos of her grandchildren exuberantly enjoying the magic of Christmas. After capturing scene after heart-warming scene including Christmas dinner with the extended family, one of her twin grandchildren knocked the tripod over, smashing the camera on the hard tile floor and particularly jarring the Microdrive.

Julia was devastated as she tried to access the photos, first in her camera, then on her notebook computer. Returning to the office glum and empty-handed, Julia shared her tale of woe while her co-workers shared their holiday snaps. Eventually someone mentioned data recovery. Although it was the first time Julia had heard of data recovery, she now knew she needed it and asked a contact at IBM for help. He pointed her to ActionFront Data Recovery Labs, a specialized service company that had impressed IBM with its ability to recover data from damaged Microdrives.

Julia called the toll-free phone number and was impressed by the confident and knowledgeable professional customer service representative and by the ActionFront customer-friendly policies of free evaluation, fair pricing, "no files = no charge" and the data guarantee. Julia sent the Microdrive to ActionFront where it was carefully analyzed and disassembled in order to read and recover the data.

Julia soon received several CDs that contained all her missing and treasured photos, and was soon showing them around the water cooler and around the country by email!

Complex Recoveries

460GB RAID5 Crash at California Technology Company
• Urgently needed for a product launch.
• Friday evening crash; recovery underway within 3 hours
• On-site and remote technicians worked around the clock.
• Complete turnaround in 36 hours!

ActionFront Data Recovery Labs launched its Critical Response Service in November 2001 to address complex data recovery situations of an urgent nature. The team had already completed a number of successful recoveries when they were called upon to restore a failed RAID server at a well-known California-based technology company.

This California-based technology company was about to launch a new product and an upgraded web service for their large installed base, to support a major marketing initiative. A large RAID 5 server needed expansion from 6 drives to 8 to increase capacity in anticipation of the enlarged user volumes. The

RAID software had never let them down, and the documentation offered them a "transparent" upgrade process. Too transparent as it turned out! After physically installing the two drives and rebuilding the RAID 5 array for the new configuration, all appeared normal.

Late that Friday afternoon, the technician rebooted and discovered to his amazement that he had lost all access to the data stored on the RAID 5 server. The tech-savvy group recognized a data loss situation, knew they needed a specialized service called "data recovery," and soon located ActionFront, by searching the web.

Nick Majors, President of ActionFront, states, "Our Critical Response Teams are on call to resolve technical crises that stump even the most qualified vendor technical support personnel. Our specialists will travel to any data center at a moments notice, and restore a failed server or rectify a failed restore operation."

Within 3 hours of speaking with a customer service representative, the ActionFront Critical Response Team was preparing the server for a step-by-step proprietary process proven to yield the best results possible in such situations. ActionFront technicians (both local and remote) worked around the clock to overcome the various unique obstacles inherent in each of these complex recoveries. By 5:00 a.m. Sunday morning, (and just 36 hours after the crash) the upgraded, expanded and well functioning data was restored and their server was back in place and ready for the marketing launch.

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 soft (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
- Regulatory requirement and obligation to patients for original data.
- Rotation errors causing erroneous EOD (End-of-Data) markers.
- IT vendor stumped or lacking resources.
- Proprietary expertise required.
- Time intensive recovery due to the nature of tape problems.

A large urban hospital in the US North East was generating approximately 90,000 medical images per day in their various clinics, requiring about 25GB of digital data storage. In order to control costs and improve efficiency, the hospital had implemented an automated, digital-tape library system for management and primary storage of the images. The system worked flawlessly serving both the clinical users as well as the related administrative staff until one day, several of the tapes appeared to be missing data or almost "empty" of data entirely. The problem was quickly traced to an inexperienced operator and did not re-occur. However the hospital had a regulatory and professional responsibility to provide integral patient care supported by the, now-lost, original images.

The tapes in question were sent to the vendor who tried repeatedly to read past the erroneous EOD markers and find the lost data. The technical support people who were well qualified to support the day-to-day issues driving customer support, did not have the right skill set and experience to solve the problem of lost data. Finally, a determined manager did some research and discovered a specialized industry segment known as "data recovery". Once she knew what to look for, she searched the web and quickly found ActionFront Data Recovery Labs. The specialists at ActionFront instantly recognized her problem, as their labs had successfully handled similar cases and had developed expertise to access these tapes when regular methods fail. ActionFront offered to review the media and quote the job under the free evaluation policy. This made it an easy decision to send the problem tape cartridges to ActionFront.

The recoveries took many hours of lab time and the cost was accordingly high, however the value of the data was even higher. The hospital was delighted to regain access to the lost images and be able to provide the high standard of health care their staff and patients demanded.

Appendix A: Data Loss Prevention

Data loss is extremely disruptive to both individuals and businesses and data recovery can be an expensive process. It is therefore in your best interest to take the time and invest the resources needed to prevent data loss. In general:

Back Up Your Systems
Whether you use a single notebook or desktop computer or are responsible for the corporate server, backing up your data is fundamental to prevent data loss. Backing up data means making a copy of critical data onto some other media and storing the back up separately from the main file set in use.

Practice Restoring from a Backup before you need it.
"My backup worked fine, however the restore did not". This is an old joke in the computer industry based on real life disasters where someone diligently used a backup routine for months or years with no hint of errors, then were unable to restore the data when they needed it. No one ever tested the backup to ensure that if it were ever needed, the restored data would be usable. Ha Ha indeed!

Never Upgrade without a Verified Backup
Before upgrading any system, perform a complete backup and restore procedure. Many data recovery cases involve upgrades gone wrong. Prove that you can quickly restore the status quo before embarking on an upgrade.

Document Your Systems
- List your applications and ensure that you are regularly backing up the data from all of them.
- Organize all original software and hardware documentation and original copies of software.

Practice Preventative Physical Maintenance
- Keep the equipment under favorable environment conditions regarding temperature and humidity.
- Install protection from power outages and power surges.
- Clean the dust from the inside or your system.
- Cleaning tape and optical drives periodically through the use of special cleaning disks and tapes.
- Take ESD precautions. (See Appendix C).

Practice Preventative Soft (Logical) Maintenance
- Delete unused/unneeded software and data files.
- Defragment your hard drive. (See Disk Defragmenter in "Windows Help").
- Perform file systems checks. (See ScanDisk, CHKDSK, FSCK in "Windows Help")
- Deploy and keep up-to-date, anti-virus and firewall software.

Pay Attention to Alarms

• Many hard drives and storage management software programs provide "self-diagnostic" utilities to warn of impending or actual failures while continuing to function. Do not ignore these warnings. For example, a RAID server may sound an alarm signaling that a drive has failed but will still serve data since built-in redundancy automatically takes over. This is intended to keep your system functioning while you replace the failing or failed component, not as a permanent solution.

Pay Attention to Security

• Are your systems adequately protected from theft or vandalism of the physical kind?
• Are your systems adequately protected from Internet hackers or disgruntled employees?

Prepare for Physical Disasters

• Take precautions to prevent or mitigate physical disasters such as fire, flood or explosions. For example, do not situate your server unprotected in a room underneath a potentially leaky plumbing pipe!
• Make a "disaster recovery plan". Where would you get the necessary equipment to bring your system back up if your current facilities were destroyed? Unfortunately, some catastrophes cannot be foreseen, prevented or mitigated.

Data Loss Prevention for Personal Users

All of the general prevention measures listed above can be used by personal computer users depending on the level of importance they assign to their data. This section recommends the simplest level of data loss prevention.

Backup

Casual personal users can simply copy important files to a floppy disk, CD or other removable media, label it appropriately and store it in case of future need, along with the original copy of any and all software programs they are using.

More sophisticated users may want to purchase a specialized backup device (such as a tape drive) or perhaps use Internet backup services to have "off-site" backup. They may want to get some help from a qualified technician to plan and implement a comprehensive backup routine.

Restore

A casual user using an informal backup method such as the one described above can simply make sure they can read the data they have made copies of.

The more sophisticated users need to document their specialized backup activities and make sure they can fully restore their system. Again, help from a qualified technician is recommended.

Data Loss Prevention for Business Users

If your business is dependant on its computer system to function, then you need to make a "business continuance plan". There are consultants and companies that specialize in this discipline if you have sophisticated needs requiring outside help. At the core of any such plan is a list of activities and resources that your business cannot be without in order to function. If you experience an emergency such as a server crash or a complete disaster, how will you keep operating? A careful reading of this Data Emergency Guide will yield many of the ideas you will need in your own business continuance plan.

Issues that particularly apply to businesses include the use of centralized servers to backup individual workstations and the need for archival (long term) storage of frequently changed data such as accounting records and databases.

Backup

For corporate mission-critical data this means setting up a structured backup procedure whereby a complete copy of all files (or sometimes just specific data files) is made, usually on a tape cartridge, and storing it off-site. Some procedures call for "incremental backup" of only the changed files, interspersed with periodic complete backups. This procedure calls for a strict rotation of clearly labeled tapes that supports a smooth restore procedure should it be necessary. Particular attention should be given to the type of backup software used to ensure full compatibility with your operating system and applications.

Restore

Any formal backup routine should be tested by a "trial restore" during the normal course of operations. If you cannot afford to risk any downtime with the system in question, try to restore the contents of that system onto an alternate or spare system. (If your application is mission-critical as this implies, then you should be maintaining an alternate in any case. See "redundancy" below.)

Redundancy

When it comes to engineering and computers, redundancy is a good thing! When a pilot thinks of a redundant engine, it is in the context that it will provide power to the aircraft, should the other engine fail.

For the largest corporations with huge financial resources, redundancy means maintaining an alternate and remote data center with an up to the minute copy of the corporate application and data. A fail-over process will automatically route all data processing activities to the alternate center during an emergency.

If your business is dependant on its computer system to function, then you need to make an investment in redundancy as part of your business continuance plan. For example, a small business will often re-purpose an older server as a workstation. Can you restore a backup to this computer and use it as the main server for a short period? A good contingency plan will identify a work-around or backup for each mission critical part of your business system.

Security
Businesses must consider both internal and external security threats of both a physical and soft (logical) nature.

Internal and external physical threats should be addressed through fire and flood proofing, and limiting access to various facilities with a high level of security surrounding a separate server room or data center.

External logical threats can be mitigated through the use of hardware and software utilities such as firewalls and virus protection.

Internal logical threats should be addressed through a comprehensive password system that assigns access rights by function. The system should be rigorously maintained and tested periodically.

Human Resources
Each organization should designate one or more individuals with the prime responsibility for data security and business continuance. This person should:
• Document the business continuance plan and have it reviewed and approved by senior management.
• Document backup and restore procedures.
• Test the restore procedures.
• Ensure compliance from the rest of the staff.
• Ensure that staff are qualified for these responsibilities and have adequate time and resources to carry them out.

Effects of Data Loss
If they are unlucky or careless, a personal user can lose countless hours of work or "priceless files" such as photos that have a high sentimental value.

For the business user, the costs can be much higher and even become a life or death issue for that business. And if a data loss situation does not actually kill a business, studies show that "downtime" costs could be in the thousands or millions of dollars per hour.

The long-term storage, maintenance and ability to use original data are formal regulatory requirements or at least a fiduciary or ethical duty in many fields. This is especially true in government, medical and financial environments.

Appendix B: Vendor Help References

Dell Corporation
http://support.dell.com/index.aspx

Fujitsu
http://www.fcpa.com/warranties/product-returns/data-recovery.html.

Fujitsu Canada
http://www.fujitsu.ca/support/hdd/data_recovery.html

**Hitachi Global Storage Technologies
(formerly IBM Storage Technology)**
http://www.hgst.com/warranty/jsp/arma24h.jsp

Maxtor
Home Page with links to support pages
http://www.maxtor.custhelp.com/cgi-bin/maxtor.cfg/php/enduser/olh_adp.php?p_faqid=719

Microsoft
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q306204

Novell
http://www.novell.com/offices/americas/canada/services_and_support.html

Seagate
General Support
http://www.seagate.com/support/kb/disc/ref/data_recovery.html
Before you return a drive checklist
http://www.seagate.com/support/npf/index.html#Reasons

Western Digital
http://www.wdc.com/support/partners/recovery.asp

Backup and Business Continuity Planning

Business continuity planning can be researched and done in-house or outsourced from a variety of vendors. There are many backup solutions comprised of various combinations of software and hardware. ActionFront does not recommend one over another.

We do recommend that you consult your preferred computer consultant or reseller and that you do your own research on the web or elsewhere.

For example try some of the following phrases on your favorite search site:
• "Backup Software"
• "Business Continuity Plan"
• "Backup over the Internet"
• "Server Backup"
• "Tape Backup"

Be sure to seek out references that have backed up and successfully restored their systems.

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.

Appendix D:
Beware DIY Solutions and Products

Beware DIY Software!

DIY (Do-It-Yourself) data recovery software may complicate your problems and diminish the prospects of a successful recovery.

The object of many DIY fix/doctor/repair programs is to try to make the drive, file-system or volume usable - not to recover existing data. Do not run any program or utility that writes to the affected media or changes it in any way, if you need your data back.

The programs that do recover data are limited to addressing assumed scenarios, not necessarily your data loss situation with its unique aspects. In contrast, ActionFront technicians have knowledgeable colleagues with 13 years of expertise to call upon, as well as proprietary software, a full range of legacy and leading edge hardware and clean rooms available.

Approximately 70% of single hard drive cases sent to ActionFront have some form of physical problem; hence the foundation of the ActionFront recovery process is making a "mirror" or copy of the media in question and performing all subsequent recovery activities on the mirrored copy. As the media in question may completely fail under repeated use, using this process increases the chances for a complete recovery and preserves the original media in case further access is required.

(You may of course purchase an additional drive and some mirroring software and attempt this process on your own if you have sufficient configuration expertise and can manage the stress in the meantime. The time and money invested in mirroring is a prelude to purchasing and running some DIY recovery software.)

Free Advice May Prove Costly!

There are numerous Internet sites offering advice about data recovery and unfortunately, the advice is often just plain wrong! Much of the advice pertains to configuration and installation issues, missing the point that most data loss situations involve the sudden inability to access data involving a previously functioning computer system or backup or the accidental erasure of data or over-writing of data control structures. Installation advice is irrelevant or harmful in these cases. Other typical errors include:
- No warning about handling and ESD issues.
- No guidance regarding what sort of noises are acceptable versus noises that indicate device failure. Drives that make "obvious mechanical fault noises" should not be repeatedly powered on and tested: it just makes them worse.

- Advice to physically manipulate a problem drive such as "twisting it quickly".
- Misleading information about Windows utilities and partitions.

The first, basic question of dealing with any media problem is "What would happen if I lost access to the data forever?" While following free advice may resolve the situation, it may severely compound the problem. Can you afford to take that risk?

If you are experiencing data loss please read this guide and consult an expert!

Appendix E:
How to Choose a Data Recovery Company

Find out whom you are dealing with:
- Who are the principals of the company?
- What are the backgrounds of key technical staff?
- What is the company's history?
- Can they offer any references?

If you are going to trust them with your valuable data, don't deal with un-named individuals hiding behind an anonymous web site.

Start out being skeptical! Even if the sales rep sounds convincing, that doesn't mean that their engineers know how to handle recoveries.

Don't be impressed by unsubstantiated claims of expertise. Some competitors falsely claim that the drive manufacturers "recommend" or "authorize" their services. Call the manufacturers directly or check the manufacturers' websites. (See Appendix B).

Don't be fooled by exaggerated claims of a 90% or 95% success rate. Data recovery can be a complicated process with inherent physical and logistical limitations that determine what can actually be done.

If you have an unusual hardware or software platform, find out if this company actually has the facilities and expertise "in-house" to handle your problem. Just because it's mentioned in their ad doesn't guarantee anything. Some services handle the simplest recoveries themselves while out-sourcing most jobs to a larger facility. Once again, ask for references!

As with any emerging field, let the buyer beware! If your data is important enough to send to a recovery service, make sure you send it to the right one.

Our Pitch

Customers with a Data Emergency Need
- Urgent Service.
- Intense Communication.
- Ability to control process.
- Pricing Integrity.
- Usable data returned to them ASAP.

ActionFront Delivers
- Critical Response goes on-site to restore mission critical operations.
- Fast turnaround for in-lab evaluations and in-lab recoveries.
- 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.
- Free evaluations.
- No files = no charge.
- Data Guarantee.
- Customer satisfaction, usable data.

Costs vs. Value
- ActionFront can estimate 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 can provide 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 Strengths
- Manufacturers support.
- 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.

ActionFront Key Benefits
- Recovery team: CSR + Lab + the Customer!
- Urgent attention to each case.
- In-lab work:
  - Free evaluations.
  - No files = no charge.
- Data Guarantee.
- Old, new and complex technology.
- Un-matched expertise gained across a wide variety of hardware/software combinations and data loss situations.
- Experience serving the most demanding customers.
- Extensive investments in the latest technology, continuous improvement in methodologies and skilled people.
- Urgent/on-site work: Critical Response Service.
- Usable Data returned to customer.

Atlanta
Technology Park
2 Sun Court
Suite 375
Norcross, GA 30092

Buffalo
(Receiving Depot)
2316 Delaware Avenue
Suite 305
Buffalo, NY 14216

Chicago
Opening Soon!

Santa Clara
3333 Bowers Avenue
Suite 235
Santa Clara, CA 95054

Toronto
340 Ferrier Street
Suite 100
Markham, ON
L3R 2Z5

Tokyo
(Service Partner)
Advanced Design Corporation
4-13, Asano-Cho
Kawasaki-Ku, Kawasaki-Shi
JAPAN
T210-0854

Toll Free: 1-800-563-1167
www.ActionFront.com

ACTION FRONT
DATA RECOVERY LABS

Toll Free: 800.563.1167 • www.ActionFront.com
Tel: 905.474.2220 • Fax: 905.944.8648

ATLANTA • BUFFALO • CHICAGO • SANTA CLARA • TORONTO • TOKYO