



Anatomy of a Data Disaster

This is an account of a real life data disaster, the background, the recovery and the consequences caused by a catastrophic failure of a production server and the company and people that it affected.

The primary file server of this company failed in the middle of the day on a Tuesday and it was apparent almost immediately that the RAID controller or backplane that handled input/output to the storage drives had failed and the viability of the data on the hard drives was questionable at best. The built-in redundancy of RAID would normally have protected the integrity of their data but the controller failure effectively scrambled the organization of almost all of the data on all drives.

Recovery efforts required a two pronged attack. The first effort would be the task of repairing the file server itself while the second area to be addressed had to be data recovery.

On day 2 the replacement parts arrived from the manufacturer and reconstruction of the server began.

The company hit its first major snag in recovery when they discovered that their off-premises corporate IT department had failed to monitor and manage the data backup system they installed for the office. The data files that were backed up were obsolete and useless and the application defined for backup had been moved from the server over a year before with no adjustments made. The email system and all office documents and communications had never been included in the backups ever. Bottom line? Their backup was worthless!

Here the efforts of data recovery and system repair collided because the tasks of reloading the O/S and software could not start until every data recovery effort on the server data had been exhausted first. Some data recovery jobs ran for 12+ hours only to recover small fractions of the lost data.

Data recovery continued through day 3. Finally, on the 4th day, the operating system, system settings and the e-mail system were re-loaded and the file server was re-installed on-site, users were reconnected to the network and basic e-mail services were restored with empty mailboxes and address books. Their entire server email system was lost.

Since there was no backup of mailboxes, rebuilding the staff mailboxes and address books began as copies of employee mailboxes were migrated back to the MS Exchange server manually from the workstations. This activity also highlighted that some users have been hoarding huge amounts of old e-mail with several mailboxes containing 40,000 e-mails or more plus attachments. The efforts to restore this much data greatly extended the time of recovery and highlighted another long term potential storage issue.

The main client and prospect data tracking system used by the sales and support staff was salvaged by the data recovery efforts but the kinks in properly re-establishing proper data ownership were still being worked out on day 5 and most of the old corrupted data files remain unusable.

For a review of the Lessons Learned, Costs and Consequences please see page 2 of this White Paper.

Anatomy of a Data Disaster - continued

Lessons Learned

Lesson #1 – RAID hard drive mirroring is not a fool-proof data protection system.

Lesson #2 – Data backups must always be monitored and verified for accuracy.

Lesson #3 – ALL processes of business must be reviewed for Disaster Recovery preparedness and appropriate fail-over alternatives must be ready to use.

Follow-up Actions

A new data backup solution is now in place with a confirmation and review process to confirm that the right data is being protected and is completing properly.

A formal Data Management review to organize and classify all company information and establish new rules for protection and retention has begun.

An e-mail indexing, archival and retrieval system to protect e-mail records is also under review.

A new contingency procedure for e-mail with links to an off-site e-mail server for temporary fail-over e-mail service is now in place.

We have created a proposal for an affordable server replication/mirroring system that will keep a real-time backup server available at a second location for the company. If the main server fails, the mirror server can be up and running within a few minutes to take over with full backup of all data, e-mail, programs and operating system.

Losses, Costs and Consequences

Lost e-mail Service - The loss of the server cut off all e-mail services to the office staff for 3+ business days really hamstrung the business operation. It's difficult to put a price tag on having no e-mail for almost 4 days but the impact on client and vendor communication had to be significant.

Data Loss - Approximately 50,000 e-mails were lost as well as hundreds of customer records, spreadsheets and documents. Hundreds of recovered spreadsheets were rendered worthless and have to be rebuilt from scratch because of formatting and formula losses.

Lost Productivity - A typical company with 40 employees spends about \$1300 per hour on employee compensation so even a reduction in productivity of 50% during the event probably cost the company between \$35-40,000 in lost productivity and overtime.

Revenue Losses - While we can't put a specific value to lost sales revenue in this case, a company with \$5 million in annual sales averages about \$2,400 per hour in revenue. The four day duration of this event put over \$76,800 of revenue at risk plus the future revenue from client business lost to the competition.

Direct Data Recovery Labor Costs – Approximately \$6,000.

Want to learn more about protecting your data and keeping your business running in an emergency?

Call ACT Network Solutions @ (847) 639-7000 or request a data security analysis by e-mailing jhoffman@act4networks.com.

*Ask about our FREE Information Management Evaluation for your business.
We'll help you determine how prepared your organization really is for a Data Disaster.*



Preparing for an IT Disaster –

Data Taxonomy and Governance -

Have you established data classification, protection and retention rules for all classes of your business data?

Established Recovery Goals -

Have you determined how long your organization can function without some or all of your IT resources?

Disaster Recovery Plan -

Do you have a written Recovery Plan that covers ALL potentialities?

Does your Recovery Plan meet your Recovery Goals for business continuity?

Data Protection -

Is ALL of your key data backed up and protected NOW?

Backup Verification -

Do you have a verification methodology in place to confirm that your data is being properly protected?

Prepare for the worst -

Do you regularly test your Disaster Recovery and Business Continuity Plan to make sure it works?



Security Solutions
Business Intelligence
Networking Infrastructure Solutions
Small Business Specialist Community