the Availability Digest

The Alaska Permanent Fund and the $38 Billion Keystroke

April 2007

Do you ever have that sinking feeling just before you depress the delete key? Am I deleting the correct file? Can I recover it if I'm wrong?

An employee of the Alaska Department of Revenue perhaps should have thought twice before acting. While maintaining a system that distributed oil revenues to Alaskans, he made that one fateful keystroke which totally wiped out an account worth $38 billion – and its backup!

The Alaska Permanent Fund

Shortly after oil from Alaska's North Slope began flowing through the Trans-Alaskan pipeline, huge revenues started flowing into the coffers of the state of Alaska. And just as quickly, this money flowed out of its coffers into the favorite projects of state politicians. Over $900 million disappeared from oil revenues in the first year.

To protect oil revenues for the citizens of the state, a state constitutional amendment was passed in 1976. It set up the Alaska Permanent Fund to receive and invest proceeds from the sale of Alaskan minerals. In 1980, the Alaska Permanent Fund Corporation was established to manage the assets of the Alaska Permanent Fund and other state funds.[1]

The Alaska Permanent Fund was set up with two goals:

- to set aside a share of oil revenues for the benefit of future generations of Alaskans after the depletion of the oil reserves, and
- to keep the oil revenues out of the hands of politicians, who could be counted on to rapidly spend it on wasteful government and extravagant capital expenditures.

The fund since then has paid a yearly dividend to all Alaskan residents. The dividends are managed by the Permanent Fund Dividend Division of the Alaska Department of Revenue. Over

[1] Wikipedia (en.wikipedia.org).

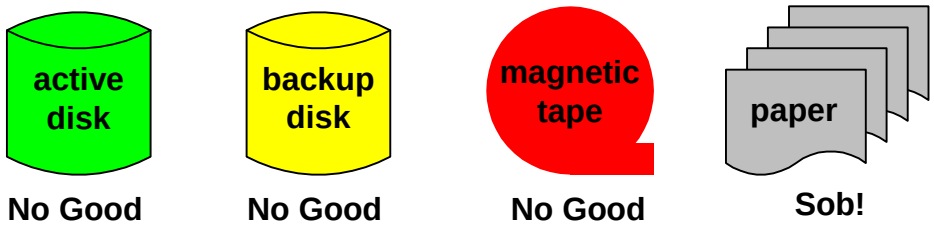
the years, annual individual dividends have ranged from $300 to $2,000 and are currently running around $1,000. The fund balance is currently about $38 billion.

The Fat Finger

On a fateful day in July, 2006, a computer technician working on a disk drive at the Department of Revenue mistakenly deleted the oil fund database, including all of the currently outstanding applicant information.[2] This was not a big problem because the data also existed on a redundant backup disk. However, under the pressure of the moment, the technician also managed to reformat the backup disk.

Not to despair. Like all good data centers, this data was backed up on magnetic tape. The only data that would be lost would be those transactions entered since the last update.

The tapes were retrieved from storage. Only then did the magnitude of the disaster become apparent. The tapes were unreadable. The triple redundancy that was built into the system was not enough. Each level of redundancy had failed. 800,000 scanned images representing transactions over the last nine months were lost.



The Painful Recovery

Over the next several days, employees of the Permanent Fund Dividend Division and the Department of Revenue, along with consultants from Microsoft and Dell, tried vainly to salvage the data. The terrible truth finally had to be accepted. The last nine months of transaction history had been lost. This included 800,000 scanned images of paper applications mailed in or filled out over the counter and supporting documentation such as birth certificates and proofs of residence.

Fortunately, there was a fourth level of backup – the paper documents themselves, stored in over 300 cardboard boxes. Each of the 800,000 documents had to be rescanned, sent through quality control, written to the database, and linked to the appropriate person's account.

It took 70 people working nights and weekends almost two months to complete the recovery, but complete it they did. To their credit, the majority of the dividend checks went out on time in October and November, including dividends to 28,000 new applicants that had not been previously processed.

Lessons Learned

We have repeatedly made the following statement. High levels of redundancy can achieve failure times measured in centuries. The probability of a failure is almost never. However, it is never zero. A failure will occur sometime, and that sometime might be tomorrow. For the Alaskan Department of Revenue, that sometime was a day in July, 2006.

[2] Much of this story is taken from an Associated Press account published by CNN.com on March 20, 2007 (www.cnn.com/2007/US/03/20/lost.data.ap/index.html).

What could they have done to reduce their chances of failure even further? Here are some ideas.

Virtual Tape

Magnetic tape backup has always suffered from several characteristics that make it somewhat unreliable. It must be transported to a backup site to ensure its availability following a disaster that takes out the site. It must be retrieved from the backup site, a procedure that could take hours or days. Once retrieved, tapes can be unreadable and totally useless for backup. This is what brought the Permanent Fund to its knees.

Today, virtual tape is a commercial reality.[3] With virtual tape, backups are made to redundant disk systems (typically RAID) rather than to tape. The virtual tape system can be remote from the processing site to provide a degree of disaster tolerance. Tapes can be spun off of the virtual tape systems if needed for regulatory or other purposes. Furthermore, virtual tape provides a much faster restore time than magnetic tape since restoration of deleted files and tables does not require searching through many (hopefully readable) magnetic tapes.

Maintenance Procedures

To allow an online disk to be reformatted or to have its data deleted is just plain folly. Proper protections should be in place to prevent a disk from being wiped out unless it is first demounted. In this case, if the technician had demounted the disk that he intended to work on, verified that the system was still running properly on the remaining disk, and then did whatever he was going to do, he would not have destroyed both disks. If he had successfully deleted the data from one disk and then had mistakenly tried to reformat the other, the request would have been denied; and he would not have taken down the system.

Operator Procedures

"When things go wrong, people get stupider" – Wendy Bartlett, HP.

As soon as the technician realized that he had mistakenly erased the first disk, you have to believe that his stress level skyrocketed. This was no time for him to continue critical maintenance. The proper procedure would have been for him to immediately stop work and call for a cohort to work with him to make sure that there would be no further operator errors. This should be a common practice in all data centers.

Test Your Backup Procedures

Backup procedures that haven't been thoroughly tested are not backup procedures at all. They are documents in a binder attracting dust.[4]

Not only should backup procedures be tested, they should be tested regularly. Configurations change. Personnel change. Procedures change.

This is especially true of tape backup procedures. Tapes themselves should be periodically tested to make sure that they are useful. For really critical data, it is not a bad idea to create two backup tape copies and to store them at separate sites. $38 billion seems to be worth that extra precaution.

[3] See Virtual Tape – The New Backup Paradigm, *Availability Digest*; November, 2006.

[4] See Don't Wait for the Other Shoe to Drop, *Availability Digest*; February, 2007.

Postscript

The recovery effort cost the state $200,000 - $128,000 for employees and $72,000 for consultants. But at least it was successful. The Department of Revenue is planning to ask the state legislature to pay this from the Permanent Fund revenues. This could mean a reduction of 37 cents in the next dividend checks. It could have been a lot worse.

The data center now has proven and regularly tested backup procedures that are much more robust.

Management was especially understanding about the situation. Not a head rolled. Former Revenue Commissioner Bill Corbus said, “Everybody felt very bad about it, and we all learned a lesson. There was no witch hunt.”