

Editorial Extract

Extracted From Paperless Ponderings
File Force International Pty Ltd
1 300 300 395 (Australia)
theboss@fileforce.com URL www.fileforce.com

Serious Records Management

SUBJECT	BACK UP OR BE DAMNED! – GET IT BACK IF YOU CAN!
Date	Extracted from Paperless Ponderings Vol 5 #6
While every effort has been made to ensure the accuracy of the attached information it is given to you as an expression of opinion of the author. File Force does not purport to be nor is it an expert on the topic. Paperless Ponderings in the periodic publication of FILEforce International © 2003	

Before anyone gets upset and says their program does the right backup, remember we have people involved. This article is all about our over willingness to rely on technology we know very little about, and presume will do it all for us.

I remember only a couple of years ago, we were cleaning up a client's office and in the fire-resistant safe discovered these slick-looking, space-age, 5 megabyte, fixed removable disks used on the then leading-edge WANG computers. (Remember them?) The label said it was the general ledger for 1997 or some similar date. The accountant said the records were very important and we had to take special precautions to make sure they were retained. The big picture thing that had been overlooked by the accountant was, not only did the company no longer have the computer that created them, but also we could almost guarantee nobody else had one either. They were subsequently trashed in the furnace after our research revealed that even if they could be read, the program that created them was also no longer available.

SOME HISTORICAL BUNGLES

That pile of 5 1/4" disks in the back of the bottom drawer of the file cabinet, or held in a fire resistant cabinet, have a probability of less than 50% of being readable, and even less chance of being useful, as you will probably not have the program enabling the use of the data file. You have upgraded, but you have probably not kept the program to replay the disk.

It's a bit like having a pile of vinyl discs and no record player to play them on. Just how many of them do you have at home?

A "backup" is the capture of data at a point in time that can allow you to replace the data relating to a PROGRAM that ran on an OPERATING SYSTEM you had at the time. So when you are looking at long-term backups or historical storage, you must be capable of re-constructing not only the data, but also the equipment, operating system and program as well. Most of you will not be able to do so.

THE MEDIA – Trust?

Yes, you have a back-up of the computer – oh yes, but, with it, can you get back to the same place you need to be at to reconstruct your records. I know it is anecdotal evidence, but I have heard too many reports of disks just not working, or the version you have saved is no longer supported at the time when the RESTORE button needs to be used. (Basically, magnetic media should be EXCITED that is USED frequently for example monthly.)

When we all had a small PC with only a 5mb drive, we always backed up because we did not have enough room for everything or we could not afford more hard drive. We regularly checked our backups, because we had to – we needed the off-line storage. Now we have "humungous" hard drive space but some of us have no backups – and if we do, they are just as unreliable as the old ones. Today, it is more important to keep copies off line but, in reality, we keep less.

WHAT DO WE DO?

Allow me to share with you what we at FILEforce do in running our Less-paper office over a VPN (Virtual Private Network). Our server contains every bit of information we need for every client job we have ever done or will be doing. This database is essential to our work.



You must, like we did, make a risk analysis of just how much data can you can afford to lose in 30 seconds due to a catastrophe such as:

- ✓ A power failure "glitch" which may lose the screen you are working on.
- ✓ A disk drive problem which can lose everything on that drive
- ✓ A fire or theft that will necessitate a major reconstruction.
- ✓ Our risk analysis convinced us to do a daily backup.

Our critical data is our CRM (Customer Relationship Manager) holds both client and human resources information, our accounting and our contract information. Our data is stored in a 24-hour facility so losing the equipment from theft is not likely.

To restore we have created CD's of the operating system, all programs, and all historical data.

To protect our daily work we have our critical data directories backed up to a data warehouse at 0500 hrs each day.

- ✓ Each week we verify our data bases
- ✓ Each month we take a CD copy for history and for the taxman.
- ✓ Each quarter we mirror-image the database for historical reasons.
- ✓ Each month we check that our backup software is working.

HOW TO BACKUP.

Once upon a time, we just had to do it ourselves. Today we have a choice. (a) back up to your own media or (b) at a specified time each day, have a data warehouse such as [SUREVAULT](#)* dial into your machine and take encrypted copies of changes to your critical data to another site. (We do it once a day, but it could be done each hour, or every other day – it depends on your risk analysis)

CHECK THAT IT WORKS

The big message of this issue is to actually check once a month that you can restore your data adequately for your needs. Yes, what I am saying is TEST IT. I have, again, heard too many stories that (a) the device did not work – ie. the media did not work, floppy did not read, CD did not read and (b) when you did restore, the time delay was so long, the lost data was of no use (fix that by more frequent backups), or (c) the stuff was not really backed up due to a code error or other software reason. (These errors can go on forever if not checked!)

CHECK YOUR BACKUP OR BE FOREVER IN DAMNATION.

60% of companies that lose their data close down within 6 months of the disaster*