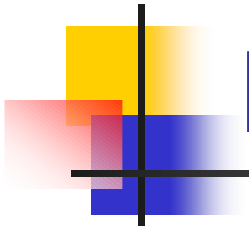
Disaster Recovery from loss of information
(Sources, Prevention, Recovery)

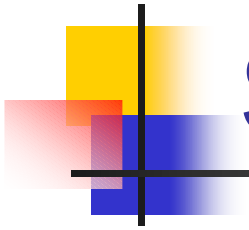
By Robert Casey

September, 2003



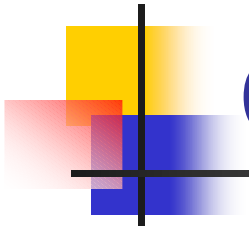
Prevention of Loss

- Reduce the probability of loss
- Backup in case of loss (CD-R)
- Incremental copies of data
- Test backup procedures



Sources of Data Loss

- User Errors (normal use) – 50 %
- Software Bugs – 20 %
- Hardware Failures – 10 %
- PC migration – 10 %
- Virus attacks – 5 %
- Theft / Fire / Floods – 5 %



Common Prevention Approaches

- Incremental saving of data
- Backup data to archive (CD-R)
- Software upgrades / patches
- Anti-virus programs
- UPS (power surges / brownouts)
- Reduce access of other casual users
- Security systems, smoke alarms

Incremental saving of data

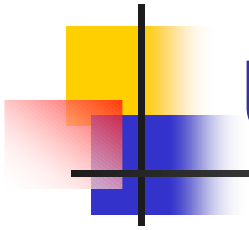
- Highest probability of saving data
- Save data under new file name
- Save every 1 or 2 hours of changes
- Delete older versions (keep latest 10)
- Use date tag or letter in file name
- BRY0503A, BRY0503B, BRY0903A

Backup data to archive (CD-R)

- Isolate data files to data directories
- Backup any data that you would miss
- GEDCOM, Word Processing, Emails
- Verify that backup worked
- Backup every few months
- Put backups far away (fire, theft)

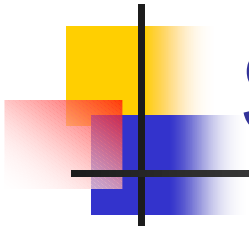
Software Upgrades / Patches

- If your software causes loss – upgrade
- Windows Fix Packs and security patches
- Entry level programs may loose data
- Don’t over-configure software profiles
- Avoid using buggy parts of programs
- Avoid too many data migrations



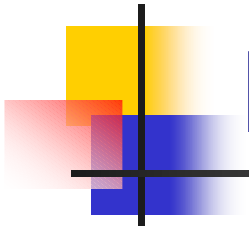
UPS (power surges / brownouts)

- Important if power is not dependable
- Inexpensive cost to avoid major loss
- Loss of data not very likely
- Loss of hard drive is catastrophic
- Power filters at minimum (vs. battery)



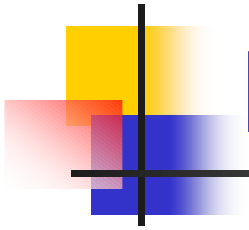
Spend time on directories

- Isolate data from different programs
- Don’t keep many copies of one image
- Rename email file every year
- Do not put 100s of files in one directory
- Create special test directories (temp)
- Separate input files from output files
- Do not mix data types too much



Different backup media

- CD-R is ideal for backup
- Diskettes hold very little
- Tape is rarely used these days
- Backup to other PC via network
- Upload to web sites (share)
- Send copies to cousins (share)

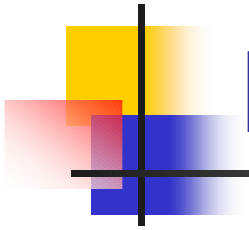


Hardware Failure Modes

- Display most vulnerable (no data loss)
- Use VGA safe mode to recover
- Power Supply vulnerable (no data loss)
- Motherboard / CPU failure can happen
- Disk can be installed in other PC’s
- Hard drive – it’s backup recovery time

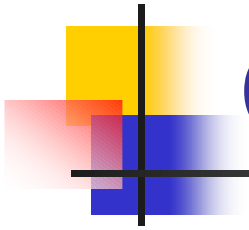
File naming conventions

- Eight character best (CD-R)
- Extension identifies data type
- Images do not need dates
- Versions of your genealogy needs dates
- Anything that you update needs dates
- Use first 3 or 4 char for line – then date



Be careful when moving data

- Copy then delete later (safer)
- Cut and then paste (not safe)
- Organizing data required (directories)
- Concept of master data very important
- External references can get corrupted
- Avoid editing same data in two sources

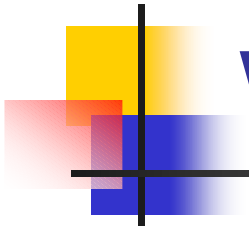


Organize data like paper files

- If you have a lot of one data, separate
- Separate by family line, geography
- Use similar method to paper files
- Avoid mixing data types (images, text)
- Data loss comes from bad organization
- Use directories like paper folders

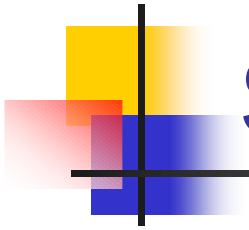
Moving data to new PC

- Use your recovery discs to move data
- Backup everything possible
- Use special programs to copy data
- If it has value – copy to new PC
- Time to delete some files – save space
- Software upgrades can corrupt data



What to backup ?

- Critical data first – genealogy
- Recent word processing files
- Recent images scanned
- Email, attachments from emails
- Some customization files if possible
- Captured web sites
- Downloaded files from Internet

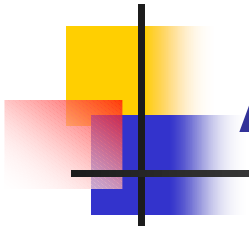


Security Systems, Smoke Alarms

- Varies depending on neighborhood
- Very expensive to implement
- Don’t leave garage open, etc.
- Store some backups offsite (fire)
- Laptops get stolen – only copies of data
- Can happen – catastrophic when occurs

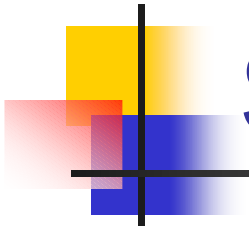
Reduce access of casual users

- Avoid children’s access to your data
- Avoid your casual use for games, etc.
- Use older or second PC’s for other uses
- May be cost-prohibitive to implement
- Older systems can still access Internet



Anti-virus programs

- Data loss is not large exposure
- Most viruses are not destructive
- Do not open email attachments (.exe)
- Keep Windows current (recent worms)
- Do not edit data when virus present
- Keep virus definitions current (1 year)



Summary

- Most data is lost by user error
- Good incremental saves very important
- Must have some backup
- Allocate time and money to odds
- Most prevention is labor
- Allocate reasonable time / funds