

Bullet Proofing Seminar Plan

Outline

- I. Presentation Goals**
 - II. Organize Your Files**
 - III. Records Back Up**
 - IV. Computer Predator Defense**
 - V. Computer Tune-up**
 - VI. Computer Automation**
-

I. Presentation Goals

Find & Plan the Implementation of Backup Tools that

- Are Free or Minimum Cost

- Are Trustworthy

- Have Proven Restoration Ability

- Are Easy to Implement

- You Can Do It Easily (*Maybe With a Little Help*)**

II. Organize Your Files

Before you can even think about creating a backup you should get your files in order.

- Not to compulsively rearrange every file in every folder

- Move essential data files are stored in one easy-to-find location (my documents)

- Move the location application of application files to my documents

Windows makes especially easy by subfolders in the documents and settings and my documents folders

Save individual software applications to a subfolder in My Documents.

Your profile also holds your personal files

- My documents folder

- Outlook express e-mail messages

- Internet explorer favorites

- Cookies

- Settings and preferences

Bullet Proofing Seminar Plan

Consider moving data files into the my documents folder to make backing up easier for software applications like

- Quicken or Microsoft money
- The master genealogist or family tree maker etc.
- TurboTax
- And more

If you're unwilling or unable to move those files at least make a note of their location to add them to the backup set later.

III. Records Back Up

Disaster planning of backups is essential to saving your genealogy and computer records

Wildfires in southern California or hurricanes in New Orleans

- How many in southern California lost their records?
- How many in New Orleans were water logged?

You can never be too prepared for catastrophe. Disaster planning of backups is essential for your data as well as knowing how to recover it

- Computer defense is essential and an absolute must in the internet world
- Careful planning of backups and virus protection will make sure you're prepared for the worst case.

Backing up essential files is neither difficult nor time-consuming

- In fact, the whole process can take as little as 10 minutes a week and windows XP does the work plan

How many backups do you think are needed?

Four are suggested

1. Hard drive failure or damaged files
2. Complete failure of your computer
3. Backup of an infected computer
4. Total loss of all records from disaster wild fire, flood, hurricane, etc.

Where would the backups be located?

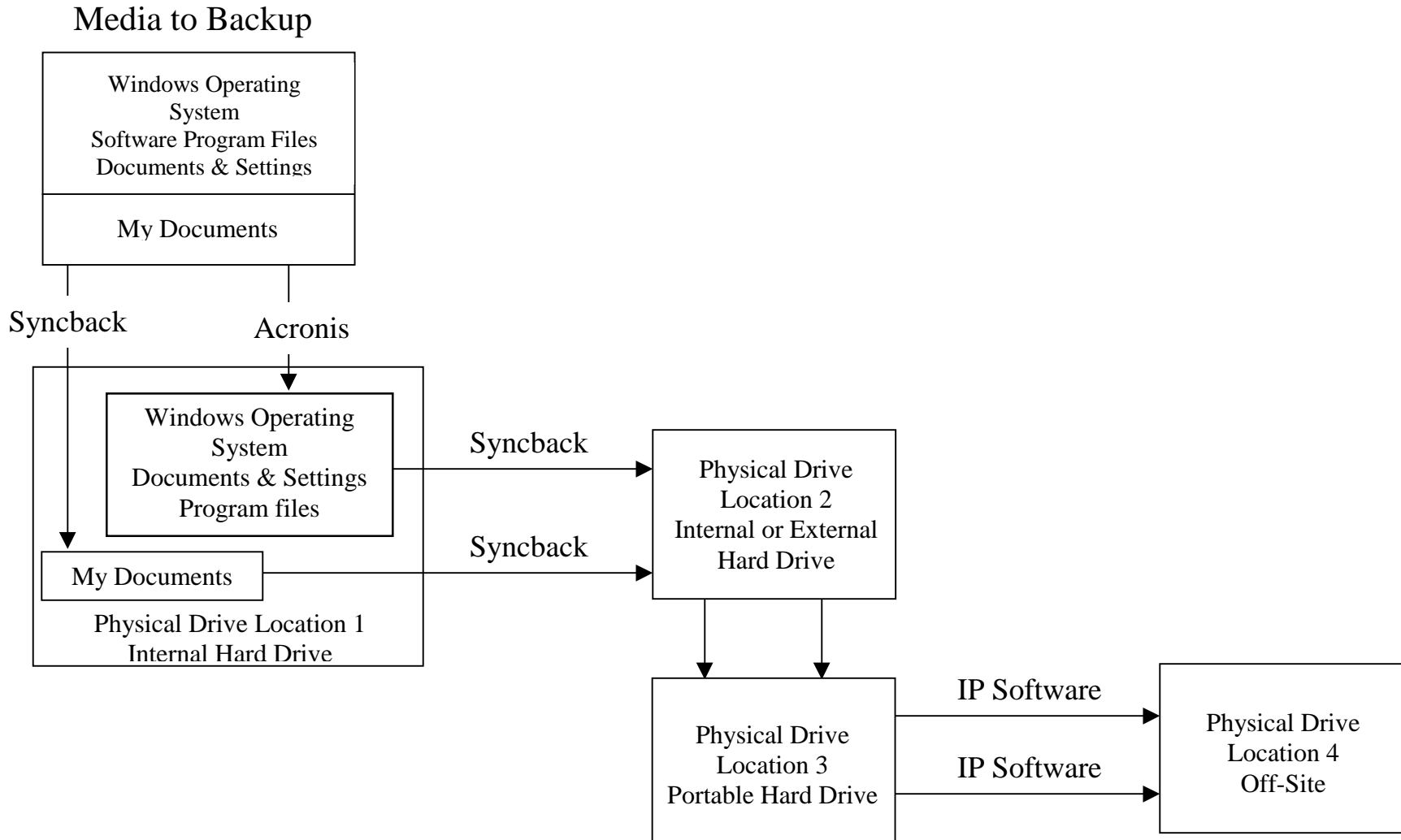
What hardware would be needed?

What software would be needed?

Bullet Proofing Seminar Plan

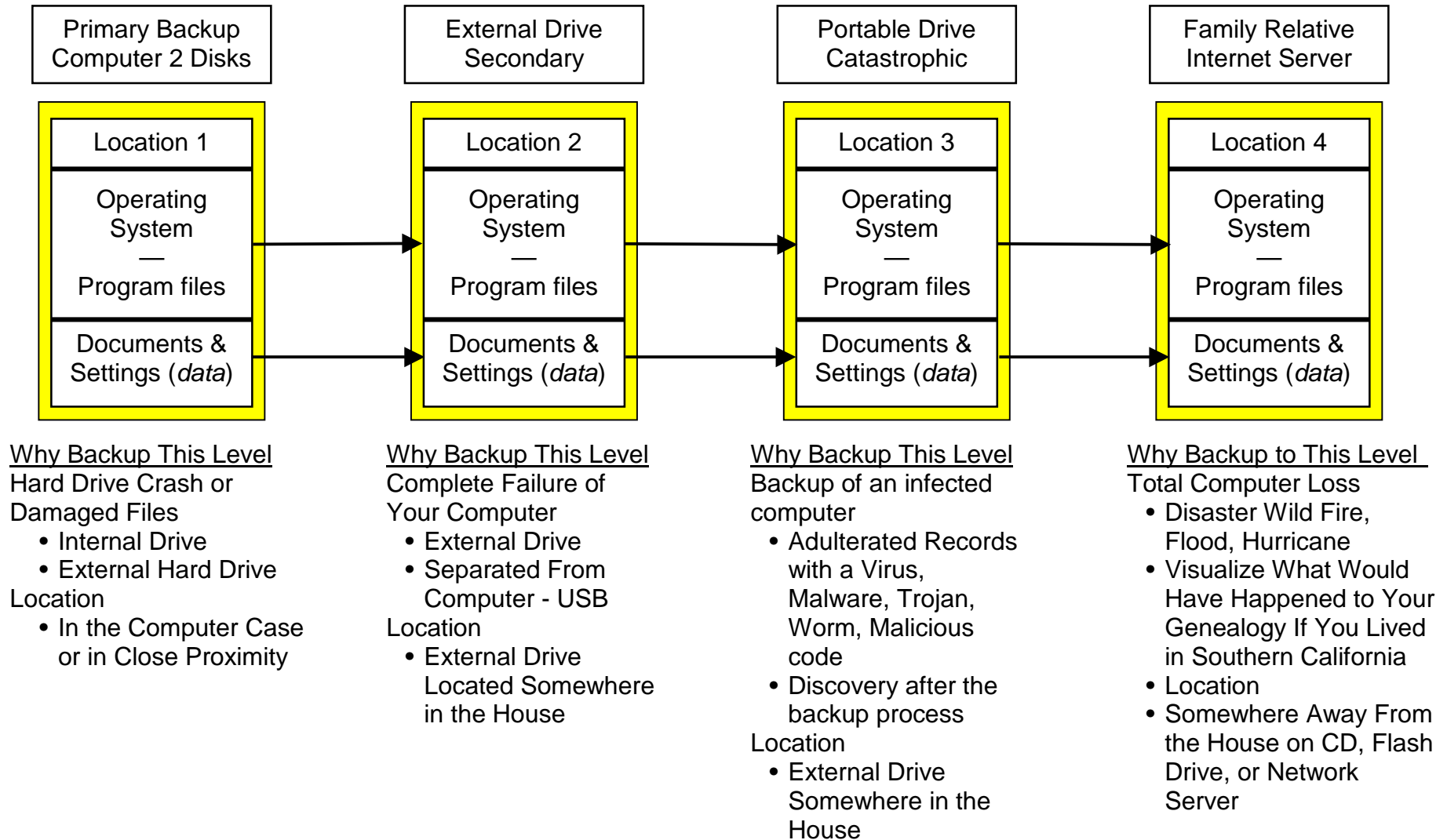
For the answer to these questions, see the schematic simplified backup system schematic on the next two pages.

Bullet Proofing Seminar Plan



Simplified Backup System Schematic, Version A

Bullet Proofing Seminar Plan



Simplified Backup System Schematic, Version B

Bullet Proofing Seminar Plan

Simplified Backup System Schematic Described

1. Hard drive crash or damaged files

Backup to an internal drive (preferred/faster)

Backup to an external hard drive

Location

In the computer case or in close proximity

Backup software

Clone Maxx

Dubaron Diskimage

Selfimage

Driveimage XML

g4u - Harddisk Image Cloning

for PCs

SystemRescueCD

Ultimate Boot CD

DiscWizard for Windows

BackupPC

Open Source Backup

Microsoft Synctoy

Unison File Synchronizer

PowerQuest Drive Image

2002

HDClone Free Edition

MaxBlast

2. Complete failure of your computer

Backup to an external drive

Separated from computer - USB

Location

Bullet Proofing Seminar Plan

External drive located somewhere in the house away from the computer

3. Backup of an infected computer

Adulterated records with a virus, malware, Trojan, worm, malicious code

Discovery after the backup process

Location

External drive somewhere in the house

Some available scanning and detection software with thousands and thousands of damaging applications attention to updating and regularly running prevention software is a must

AD-Aware

AVG Updater

AVG

AVG Free Edition

Update Service

AVG Anti-Root Kit

Advanced Disk Cleaner

Windows Defender

Windows Malware Removal

Windows Malicious Software

Removal Tool

SpyBot Updates

SpyBot S&D

SpyBot Tea Timer

Spyware Blaster

Spyware Blaster Update

Panda

McAfee

Norton

Windows Firewall

Bullet Proofing Seminar Plan

Network Router Firewall

4. Total Computer Loss

Disaster wild fire, flood, hurricane

Visualize what would have happened to your genealogy if you lived in southern California

Location

Somewhere away from the house on cd, flash drive, or network Server

Top Online Backup Services

MediaMax

OmniDrive

Mozy

Carbonite

More with a search

Records Backup - Online Backup Services

The major concern of security of data on their system should not be a problem since most offer encryption and strict permission security features for gateway access

Several have storage up to 100 GB and at reasonable prices and some are free

In most cases you may only back up your entire system once a week

Incremental backups more often

In most cases important files once a week or once a day, depending on how often the files are changed • after your files are upload

Bullet Proofing Seminar Plan

IV. Computer Predators Defense

Surfing the Internet Can Be Dangerous Unless Your Protected From Dialers

Programs often used to maliciously redirect Internet connections

When used it disconnects the legitimate telephone connection used to connect to the Internet and reconnects via a premium rate number (1-900 numbers)

Often, the first indication a user has of this activity is an extremely expensive phone bill,

Malicious dialer programs are a type of spyware that can install itself to your dial-up settings.

Hackers/Crackers

Individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data. Hackers, themselves, maintain that the proper term for such individuals is a Crackers

Malware

Short for malicious software, software designed specifically to damage or disrupt a system, such as a virus or a Trojan horse

Spyware

Software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes

Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet

The majority of freeware and shareware applications do not come with spyware

Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else

Spyware can also gather information about e-mail addresses and even passwords and credit card numbers

Trojans

Bullet Proofing Seminar Plan

A destructive program that masquerades as a benign application. Unlike virus, Trojan horses do not replicate themselves but they can be just as destructive

One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer

Viruses

A program or piece of computer code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves

All computer viruses are manmade

A simple virus that can make a copy of itself over and over again is relatively easy to produce

Even a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt

A more dangerous virus is one capable of transmitting itself across networks and bypassing security systems

Phishing

Sending an e-mail to a user falsely claiming to be an established legitimate enterprise to scam the user into surrendering private information used for identity theft

The e-mail directs the user to visit a website where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers

No legitimate organization will ask for it

The web site, however, is bogus and set up only to steal the user's information

V. Computer Tune-up

Tools That Improve Computer Performance

De-fragment all disks

Routinely remove temporary files

VI. Computer Automation

Automating backup of genealogy records and operating system

Bullet Proofing Seminar Plan

Automatic update of damage control software

Automating scans for dialers, hackers, malware, spybots, trojans, viruses & phishing

Automating computer tune-up

SET IT AND FORGET IT (almost)

If you're disciplined enough, you can repeat the above steps once each week and perform regular backups whenever you're ready.

If you'd rather not count on remembering to perform this crucial task, however, set up an automatic backup schedule for windows.

Automation of the backup and scanning actions is accomplished by windows resident

Task scheduling capability

Hibernation (& standby)

Automation should be run at a time when you are not using the computer

The actions can take up most of the computers processing capability

Better overnight

Leaving the power on is a choice

Powering down PC components is counterproductive because of the effect on component life

Other things being equal, electronic components are more stable and don't have electrical loading and running temperature at startup

Use windows XP's hibernation feature on your computer to put your system to sleep at the end of the day rather turning it off

Your system can be made to "wake up" to run the backup and scanning tasks you've scheduled

How to set up this schedule will be explained in the workshop