Protecting Your Data

COMP620

“What does a computer hard disk and a gerbil have in common? Their average lifespan is about 3-5 years.”

T.E. Ronneberg

Schedule

Monday, November 12 System Protection	Wednesday, November 14 Check Point Software Technologies	Friday, November 16 Review for exam
Monday, November 19 Exam 3	Wednesday, November 21 Thanksgiving Holiday (no classes)	Friday, November 23 Thanksgiving Holiday (no classes)
Monday, November 26 review for final exam	Wednesday, November 28 Final Lecture	Saturday, December 1 10:00am – 12:00pm Final Exam

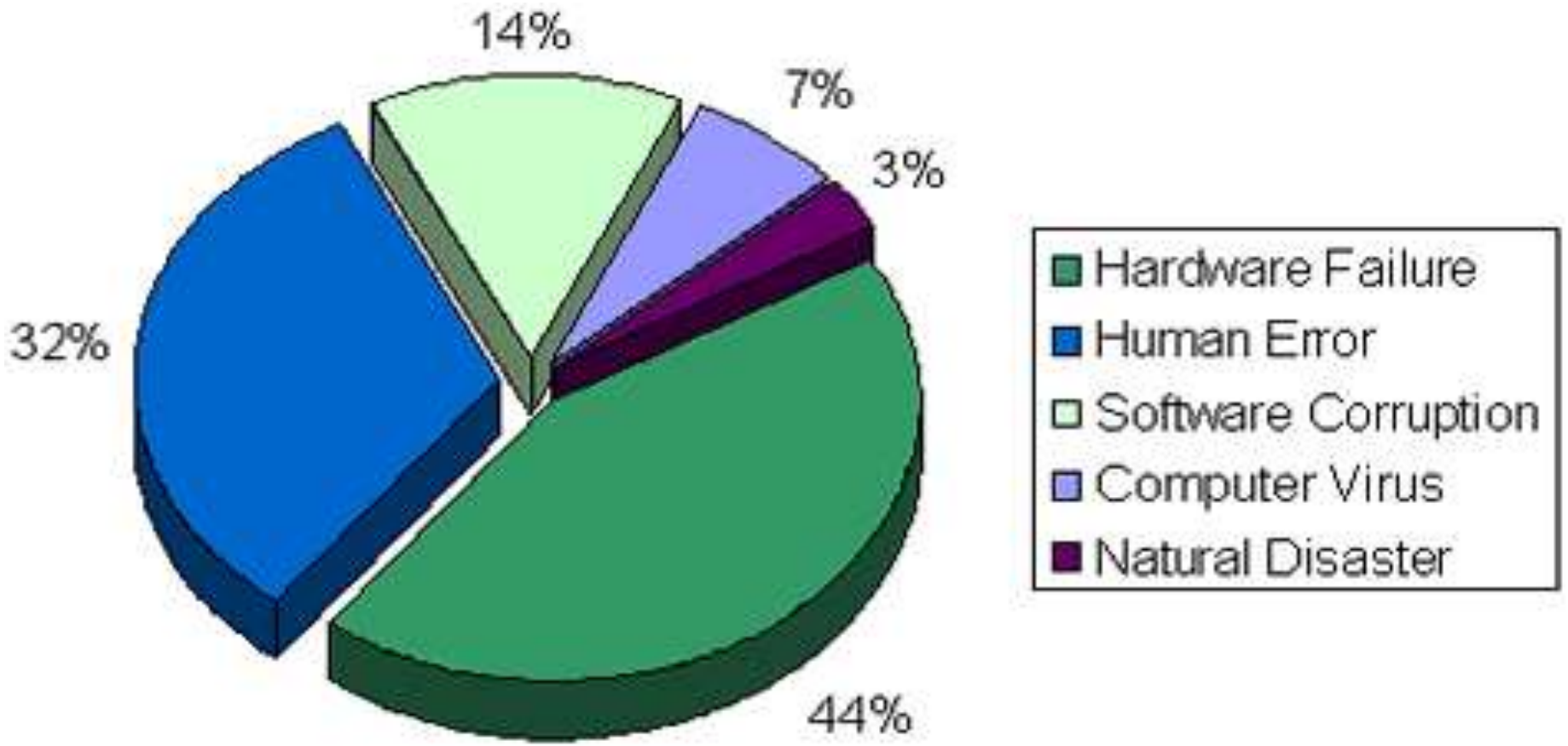
Your Disk Will Die!

It is a matter of **when**, not **if**

Types of Data Loss

- User error (accidental deletion, lose CD, forget password, etc.)
- Disk failure
- Data corruption (file system failure)
- OS failure
- Power failure (cached data not saved)
- Natural disaster (fire, flood, plague of locust)
- Malware
- Theft of equipment

Causes of Data Loss



Information Assurance

It is less probable that somebody else will destroy your data than you will lose your data all by yourself

When you use your computer, where do you usually store your data?

A. Hard drive
B. USB thumb drive
C. External hard drive
D. other

When was the last time you backed up the data on your computer?

A. Sooner than a week ago
B. One week ago
C. One month ago
D. Longer than a month
E. Never

When was the last time you backed up your phone?

A. Sooner than a week ago
B. One week ago
C. One month ago
D. Longer than a month
E. Never

Have you ever lost your data?

A. Never

B. Once

C. Several times

D. Many times

Cost of Data

- How much can you afford to lose?
- Backup often enough so that you can afford to lose the data since the last backup
- Many users can easily recover with daily backups. Some systems need immediate backups

Risk Analysis

Consider

- The cost of the loss of data
- The cost of backing up your data
- The probability that a failure will occur over a period of time

Saving to Disk

- When you are working on something, be sure to save the results to disk every so often
- If there is a failure, how much work can you stand to lose
- Always save your information when you step away from your computer
- It just takes a click

“Back up my hard drive? How do I put it in reverse?”

Concurrent Backup

- Some systems are very concerned about losing data
- Every update is transmitted to a remote backup facility as it is made
- Database audit trails record all changes made to the database

RAID

- **R**edundant **A**rray of **I**ndependent **D**isks
- A collection of disks are used as one large unit of mass storage
- Multiple disks operating simultaneously can increase the data transfer rate
- Extra data stored on the disks can recover the information should a disk fail

RAID Comparison

RAID	Disks	Reads	Writes	Survives failures
0	N	faster	faster	0
1	2N	slightly faster	slightly slower	1
5	N+1	faster	slightly slower	1
6	N+2	faster	slightly slower	2

Disk Failure Only

- RAID 1 – 6 will improve disk hardware reliability
- Most data loss is not the result of hardware failure
- If the user or software deletes a file, the hardware will dutifully delete it from all disks in a RAID bank
- Failure of the disk controller will leave unreadable disks

Common Backup Scheme

- Backup all data on a quarterly basis *(possibly more or less frequently)*
- Do incremental backups of new and modified files daily

Backup Media Considerations

- Cost
- Speed
  - Data transfer rate
  - Ability to restore an individual file
- Reliability
- Volume
- Life span

Backup Devices

- CD – read-only units of 600-750 MB
- DVD-R – read-only units of 4.7 GB
- DVD-RW – rewritable in units of 4.7 GB
- USB memory sticks – expensive
- Remote server – initially expense, but effective
- External hard drive - initial expense, but effective
- Commercial cloud – reoccurring expense, but reliable

- Tapes – slow and unreliable

Backup Data Storage

- Removable backup media should not be stored near the computer. A disaster destroying the computer will destroy the backups
- It should not be too difficult to retrieve the backup media in case a file needs to be restored

Saving the Backups

- We used to do an incremental backup of a mainframe system every day at 3:00am
- Friday nights we did a full backup
- The previous weeks tapes were stored in the vault of a local bank

Sad Story

- A graduate student was almost finished with his thesis
- He carefully backed up his work every day to floppy disks and stored the labeled floppy disks in a box next to the computer
- A thief stole his computer and also took the box of floppies

Security

- Your backup media might be sitting on a shelf while your computer is locked away
- Your data can be read from your backup files
- If someone can change your backups and then force a restore, they can change the data on your computer
- Encryption can help protect backup data

Cloud Backups

- There are many companies that sell backup services
- Backup programs start on a regular schedule and backup your data over the network to a remote system

Top 3 things to do to keep your computer safe from attack

- Write a short list of 3 things everyone should do to keep your computer safe

My Top Ten Recommendations

1. Anti-virus – Install an anti-virus program
   – Configure it for automatic signature updates
2. NAT – Network Address Translation will protect outside systems from connecting to your computers
3. Firewall – Either on the computer or your router
4. Disable autorun – When you insert a thumb drive or CD, your computer can automatically start executing software on the device. Do not allow this

My Top Ten Recommendations

5. Use strong passwords
   - Passwords need to be long and random
   - You need to be able to remember them
   - Try using phrases
6. Install security updates – Keep your system up to date
7. Delete programs that start at logon
   - If you don’t need it, it shouldn’t start automatically

My Top Ten Recommendations

8. Don’t allow phone apps access they don’t need
   - Apps from the store may not be safe
   - Do not allow them access that is not core to their purpose
9. Watch for browser plugins
   - If you don’t use it, don’t have it installed
10. Watch for Phishing
   - Inappropriate return address
   - Generic
   - Poor grammar

What Did I Miss?

Protecting Ourselves

- It doesn’t take a malicious hacker to make you lose your data
- You can do it all by yourself

Schedule

Monday, November 12 System Protection	Wednesday, November 14 Check Point Software Technologies	Friday, November 16 Review for exam
Monday, November 19 Exam 3	Wednesday, November 21 Thanksgiving Holiday (no classes)	Friday, November 23 Thanksgiving Holiday (no classes)
Monday, November 26 review for final exam	Wednesday, November 28 Final Lecture	Saturday, December 1 10:00am – 12:00pm Final Exam