Data Loss Prevention (DLP) & Recovery Methodologies

Topics to be Discussed

- Overview of Types of Storage Devices
- Prevention Methodologies on storage devices
- Creating a Backup Plan
- Testing your Recovery Plan
- Backup Software List
- Performing Level-1 Recoveries on Hard Disks

Storage Device Overview

- Storages Devices

Storage Devices

- Local Hard Disk Storage (Internal)
  - Interface: SATA
  - Single Drive Configuration (Spindle or SSD)
  - SATA or SAS Style RAID Configuration
- External Hard Disk or Flash Based Storage
  - HDD Interface: USB 2.0/3.0, eSATA, Firewire, Thunderbolt
  - Flash Interface: USB 2.0/3.0
- Network Attached Storage (NAS) (External)
  - Type: Single Disk or RAID (0, 1, 0+1, 5, 6)
  - Interface: 10/100/1000 Ethernet Port
- Cloud Based Services (Client/Server)
  - Amazon, Dropbox, Carbonite, CrashPlan, etc.
- Internal/External Tape or Optical Devices
  - Media: LTO, DLT, SDLT, AIT, VXA, 8MM, Linear Tape File System (LTFS)

Prevention Overview

- Prevention Methodologies “Hardware”
  - Desktop-Laptop Computers
  - Flash Based Devices
  - NAS Devices
  - Tape Devices

Prevention Methodologies "Hardware"

- Desktop-Laptop Computers
  - The internal drive should be large enough to store ALL your data with room for growth.
  - Have a second internal hard drive.
  - Have an external hard drive or NAS that is larger than the internal hard drive.
  - Have a second external hard drive.

- Rule 1: If the data is only in one location then you have no backup!

- Story time of Epic Failure:
  - My external hard drive was booting slow and had errors copying files

Prevention Continued

- Flash Based Devices
  - Using Flash devices to transport data
    - Always do your work on your main system
    - Copy your data to the Flash Drive
    - Copy the data from the Flash Drive to the Target system
    - Do the work on the Target system
    - Copy your data from the Target system to the Flash drive
    - Copy the data from the Flash Drive to the main system
  - Option 2
    - Have (2) Flash drives – Copy the data twice so just in case one fails!

- Rule 2: When a flash drive fails it will be at the move critical time!
- Story time of Epic Failure:
  - USB 3.0 Flash - QuickBooks data

Prevention Continued

- NAS / SAN Devices
  - Configured using RAID 5 or 6
  - Multiple NAS Sync functionality
  - Export data to tape

- Story time of Epic Failure:
  - Local disk near full and the Drobo RAID

Prevention Continued

- Tape Devices
  - Long-term storage – allows snapshots of data over a long period of time without having it on-line.
  - Data deduplication – addresses the exploding data growth through the identification an elimination of redundant data.
  - Automation – increase efficiency and agility in managing backup and recovery infrastructure.

- Story time of Epic Failure:
  - The Tape Backup that never happened – Doctors office

Backup and Recovery Planning

- Creating a Backup Plan
- Figuring Out a Backup Plan
- The Basic Type of Backups
- Selecting Backup Devices and Media
- Common Backup Solutions
- Pro’s of Backup Solutions
- Con’s of Backup Solutions
- Testing your Recovery Plan

Creating a Backup Plan

- Data backup is an insurance plan. Important files are accidentally deleted all the time. Mission-critical data can become corrupt. Natural disasters can leave your office in ruin. With a solid backup and recovery plan, you can recover from any of these. Without one, you're left with nothing to fall back on.

- Rule 3: When S**T happens it is cheaper to have two forms of backups then one. The time, costs, and legal problems can be mitigated if you make an investment at the start then allow for growth!

Figuring Out a Backup Plan

- It takes time to create and implement a backup and recovery plan. You'll need to figure out what data needs to be backed up, how often the data should be backed up, and more. To help you create a plan, consider the following:

This is the Who, What, Where and Why with a little bit of How!

- Who will be responsible for the backup and recovery plan?
- How important is the data on your systems?
- What type of information does the data contain?
- How often does the data change?
- How quickly do you need to recover the data?
- Do you have the software or equipment to perform backups?
- What is the best time to schedule backups?
- Do you need to store backups off-site?
- What structure will the data take before the backup and during the restore?

The Basic Types of Backups

- **Normal/full backups** - All files that have been selected are backed up, regardless of the setting of the archive attribute. When a file is backed up, the archive attribute is cleared. If the file is later modified, this attribute is set, which indicates that the file needs to be backed up.

- **Copy backups** - All files that have been selected are backed up, regardless of the setting of the archive attribute. Unlike a normal backup, the archive attribute on files isn't modified. This allows you to perform other types of backups on the files at a later date.

- **Differential backups** - Designed to create backup copies of files that have changed since the last normal backup. The presence of the archive attribute indicates that the file has been modified and only files with this attribute are backed up. However, the archive attribute on files isn't modified. This allows you to perform other types of backups on the files at a later date.

- **Incremental backups** - Designed to create backups of files that have changed since the most recent normal or incremental backup. The presence of the archive attribute indicates that the file has been modified and only files with this attribute are backed up. When a file is backed up, the archive attribute is cleared. If the file is later modified, this attribute is set, which indicates that the file needs to be backed up.

- **Daily backups** Designed to back up files using the modification date on the file itself. If a file has been modified on the same day as the backup, the file will be backed up. This technique doesn't change the archive attributes of files.

Basic Types of Backups

- **Real-Time Backups** This backup is designed to watch folder / files and immediately upon change!

- **Virtual Machines or Imaging** – Designed to backup entire machines, settings, and environment.

Selecting Backup Devices and Media

- Many tools are available for backing up data. Some are fast and expensive. Others are slow but very reliable. The backup solution that's right for your organization depends on many factors, including:

- **Capacity** - The amount of data that you need to back up on a routine basis. Can the backup hardware support the required load given your time and resource constraints?
- **Reliability** - The reliability of the backup hardware and media. Can you afford to sacrifice reliability to meet budget or time needs?
- **Extensibility** - The extensibility of the backup solution. Will this solution meet your needs as the organization grows?
- **Speed** - The speed with which data can be backed up and recovered. Can you afford to sacrifice speed to reduce costs?
- **Cost - *The cost of the backup solution. Does it fit into your budget?***

Common Backup Solutions

- Capacity, reliability, extensibility, speed, and cost are the issues driving your backup plan. If you understand how these issues affect your organization, you'll be on track to select an appropriate backup solution. Some of the most commonly used backup solutions include:

- **Disk drives (in system backup drive)**
- **External media device (DAS, NAS)**
- **SAN / NAS Appliances ($$)**
- **Tape Devices ($)**
  - Auto-loader library tape systems
  - Linear Tape File System (LTFS)
- **Cloud Based Services ($)**
  - Upload costs very from Download costs due to bandwidth usage and service purchased.

Pro's of Backup Solutions

- **Hard Disk, DAS, NAS, SAN ($$)**
  - Restoration can be done in a short amount of time
  - Media cost per Terabyte is reasonable
  - Scalable architecture which allows storage systems to always available
- **Tape Devices ($)**
  - Automated through both hardware and software
  - Scalable archiving for current and Long-term Storage
  - Per tape cost is cheaper
    - LTO 5 @ $23.95/tape (1.5/3.0TB) or LTO 6 @ $51/tape (2.5TB/6.25TB)
- **Cloud Based Services ($)**
  - Can be accessed anywhere, anytime.
  - Automated backup through software

Con's of Backup Solutions

- **Hard Disk, DAS, NAS, SAN ($$)**
  - Media and equipment hardware failure, upfront infrastructure costs, maintenance contracts, monthly power bill
- **Tape Devices ($)**
  - Media and equipment hardware failure, upfront infrastructure costs, maintenance contracts, monthly power bill
- **Cloud Based Services ($)**
  - Monthly Access & Service Fees;
  - Not in your control; means Forget to pay = NO ACCESS, NO DATA
  - Download bandwidth costs can be higher that upload costs.
  - TNO compliance

Testing your Recovery Plan

- Nothing is more important to have the ability to restore what you have backed up! This is the most overlooked portion for the DLP process.
  - Backup and Restore process that is untested can lead you to not being able to restore any data, depending upon the media or container, back to a usable form when needed.
  - Testing will show where the weakest link or links may be!

- Rule 4: Test, Check, Observe, and do it again! Repetition will allow you to get your systems back up and running and have the shortest downtime.

Backup Software

- Commercial / Proprietary and Freeware
- https://en.wikipedia.org/wiki/List_of_backup_software

- This list covers ALL OS's with other stats.
  - Windows
  - Linux
  - MAC OSX

- Note: The Wiki page is a great place to start but it by no means does not contain all available backup software!

Performing Level-1 Recoveries on Hard Disks

- Identifying the problem
- Recovery Software

Identifying the problem

- Common Level-1 Indicators
  - Drive boots slower over time
  - While booting you get (BIOS or OS)
    - BSOD's but clear up after reboot!
    - Continuous BSOD's
    - An error message saying your disk is not bootable
    - One or more boot files may be missing or damaged
  - Random errors while copying files
  - Attached external needs to be formatted

Top Rated Recovery Software

- Proprietary / Commercial
  - 1. File Scavenger
    - Windows: NTFS, FAT32, FAT16, exFAT
    - Linux: Ext3, Ext4, UFS1, UFS2, XFS.
    - Apple: HFS+
    - Virtual file systems: VMFS, VMDK, VHD and VHDX
  - 2. R-Studio
    - Windows: FAT/NTFS, exFAT
    - Resilient File System: ReFS,
    - Mac: HFS/HFS+
    - Linux: UFS1/UFS2 & Ext2FS/3FS/4FS
    - Reverse RAIDs support

Recovery Software Cont.

- Proprietary / Commercial
  - 3. GetDataBack
    - Windows: FAT/NTFS
  - 4. Mac Boot CD/DVD ($)
  - 5. Windows Vista/7/8 Rescue Boot CD ($)
- Free Software – Track0, Partition, OS Structure
  - Hiren's Boot CD/DVD
  - Ultimate Boot CD
  - Linux Boot CD/DVD

You have reached the End