Data Backup and Disaster Recovery

Module 5

Simplifying Security.

Certified Secure Computer User

Module 5: Data Backup and Disaster Recovery

Exam 112-12

Module Objective

Computers store a lot of data gathered by users. But a system crash or theft may result in the loss of all that data. To avoid this, **copies of critical data** should be made frequently. This module talks about securing files and how to back up the critical data.

This module will familiarize you with:

- Data Backup
- What Files to Backup and How Often?
- Online Data Backup
- Online Backup Service Providers
- Types of Backup
- Windows 7: Backup and Restore
- Data Encryption
- MAC OS X: Backup and Restore
- Data Backup Tools
- Data Recovery Tools
- Physical Security
- Physical Security Measures
- Laptop Theft
- Physical Security Checklist

Module Flow

Data Backup Introduction

Windows 7 Backup and Restore

Data Encryption

MAC OS X Backup and Restore

Data Backup Tools

Data Recovery Tools

Physical Security

Data Backup

Backup refers to making **duplicate copies** of data that may be used for recovery after a disaster or damage to the data. Data backup should be the top priority in computer maintenance along with virus protection. Backup is required in case a file or group of files is lost. Its main purpose is to create additional copies of data stored in the computer to be used to **restore** the original **after a data loss** event.

The user should back up critical information that cannot be easily replaced. For example, files or documents such as financial documents, bank records, software or assets purchased, marketing strategy documents, etc. should be backed up.

Critical information should be backed up on a regular basis, and the copies of those files must be placed in another location.

Need for Backup

Data can be lost in many different ways, such as **application errors** in the software, configuration errors, or even a **natural disaster**. Data backup ensures that the data is secure in case of a **disaster**. It is **easy** and **cost-effective** to back up data compared with **recovering** the data after a disaster or system crash.

Most users have come across situations in which their systems or laptops had crashed. Users may even **lose the media** on which they stored years' worth of work documents, bank account information, personal photos, videos, and email messages.

It is, therefore, important that the user makes backup copies of all his or her data to avoid losing it and to **prepare for emergencies**.

The main purpose of backups is:

- To **restore critical data** after data loss. A disaster may lead to the loss of critical information, but if the information has a backup copy, it would restore the information.
- To restore files when they are **accidentally deleted** or **corrupted**. Due to improper password handling or during transmission/storage, it is possible for the files to be corrupted or deleted. This discards the request of accessing files by the authorized party. If this occurs, backup would be an advantage and would help in restoring those files.
- In addition, backup can also be used to access **older versions of files** after changes have been made in the current version.

Types of Data Loss

Natural Disaster:

Data loss can result from floods, fire, hurricanes, and power surges. It is recommended to keep data in two different locations as it is unlikely for natural disasters to occur in two separate locations.

Human Error:

Human errors include **unintended deletions**, accidental formatting of the hard drive, and mistakes on the part of the administrator or management information system (MIS) department. Knowledge of basic computer operation will limit this risk.

Corrupt File System:

The file system manages all the files and directories on hard drive. Buggy software, **virus infections**, human errors, processor overclocking, and unexpected system shutdown are the main reasons for file corruption. Use a suitable utility for the OS version in use to reduce risk.

Software Corruption:

An operating system may have a write error or **memory error** that causes the software to crash. For example, if a word processing program crashes, the unsaved data will be lost. To overcome the risk, periodically save the data as it is being entered.

Computer Virus:

Malware such as Trojans and viruses cause data loss or make data unusable. Computers are infected with viruses when **software containing virus** files is installed or when files are downloaded from a malicious website. Use of anti-spyware and anti-virus software reduce this risk of data loss.

Hardware Malfunction:

Hardware malfunction results from controller failure, **media crash**, and power failure. Errors with the hard disk drive are the most typical type of hardware problem.

Symptoms include:

- An error message stating device unrecognized
- The hard drive may not rotate
- A rattling or scraping sound
- The system or hard drive cannot operate
- Loss of data accessed previously

What Files to Backup and How Often?

The user should first **decide** which information needs backup and which does not. Backing up all information only **increases the cost** of backup and the **time required** for recovery. It may also make data recovery confusing for the user. The user has to decide what data is critical and needs to be backed up. Some files and documents a user would want to back up include:

- Operating system files purchased with the computer, CDs, software, etc.
- Important office documents
- Software downloaded (purchased) from the Internet
- Contact information (email address book)
- Personal photos, music, and videos

Data loss can be prevented by backing up on a **daily basis**. But backing up everything daily can be costly and time consuming, so it is important to identify only the data that changes.

It is always recommended to **back up files regularly**. The user should back up whenever any changes are made to the important files, so that the user has the latest copy available even if the original one is lost/ damaged. Schedule backup software to copy files on a predetermined day (example: every Monday). Essentially, every file or item that undergoes changes since the last backup should be backed up.

Online Data Backup

Data can be backed up using the Internet. There are two types of online data backup:

- **Download and install** software provided by an online backup service provider, connect it to the server of the service provider, choose the files to backup, and transfer to that server. When required, restore from the backup stored on that server.
- Choose a **web-based** online data backup service from the browser window. This allows you to access your stored data from any system with an Internet connection.

Advantages of Online Data Backup:

- **Offsite storage** offers disaster recovery.
- Users do not have to purchase new equipment.
- There are no ongoing staff costs or media costs, only running costs that are paid monthly.
- It is **easy** to install and setup.
- It ensures the security of data (software collects the files, compresses, encrypts, and then transfers the data to the remote backup service provider's servers).
- **Data recovery is fast** and can be accessed from anywhere in the world.

Online Backup Service Providers

Online backup service providers, also known as **remote or managed backup services**, are the companies that provide users with a system for backing up and storing computer files. Advantages of the online backup service providers include:

- Aid from virus attacks
- Ability to coordinate and manage stored data from anywhere in the world
- Flawless speed in terms of restoration and backup processes
- Real-time backup

Online Backup Service Providers

- **Carbonite** (http://www.carbonite.com)
- **SpiderOak** (https://spideroak.com)
- **IDrive** (https://www.idrive.com)
- **Acronis** (http://www.acronis.com)
- **Mozy** (https://mozy.com)
- **SafeCopy** (http://www.safecopybackup.com)
- **Jungledisk** (http://www.paragon-software.com)
- **SugarSync** (http://www.sugarsync.com)
- **Memopal** (http://memopal.com)
- **ElephantDrive** (http://www.elephantdrive.com)
- **SOS Online Backup** (http://www.sosonlinebackup.com)

Types of Backup

Full backups: Full backups run for **complete data** on all the systems during the weekend. For example, if the backup is performed on 10 TB data, then all 10 TB will be written to a set of 10 tapes every weekend.

A few applications such as database or email data might be backed up nightly as a full backup. Nightly backup is performed as the process consumes large network bandwidth and various other resources that might degrade network speed.

Normal backups: Normal backups include only the files that are marked and deemed necessary by the user.

Incremental backups: Incremental backups back up the files that have been changed after the last full backup (i.e., it is a daily backup of each file on a system that has been changed since the last backup). Although performing incremental backups is easy compared with others, restoration using these backups is time consuming as the process follows a **sequential approach**.

For example, if the last full backup was performed on a Saturday, then the files that are changed on Monday, Tuesday, and Wednesday would be backed up using increment backup.

Differential backups: A differential backup backs up every file on a system that has been altered after the last full backup. It reduces the time for restoring files that are backed up during the week. For example, if the full backup is performed on Sunday, the differential backup would be performed on Monday, Tuesday, Wednesday, and Thursday.

Running differential backup on week days could make the personnel at an organization concentrate only on the backup process, which may result in confusion with a **large number of backups**. To overcome this, differential backups are performed once or twice a week.

Back Up the Data Using Windows Backup

The Windows backup utility allows users to **protect data** by creating a duplicate copy of the files and folders on the hard disk and then archive to an external storage device (such as a hard disk or tape). If the original hard disk is erased accidentally, becomes inaccessible, or is overwritten due to a malfunction, then the user can restore the archived copy of data using **Automated System Recovery Wizard** or **Restore Wizard**. Files are restored to their previous positions after restoring the backup data.

Windows also allows users to create a **restoration point**. If the system is infected by malware, the user can choose to restore the computer to a restore point before the computer was infected.

Steps to Backup Data

Source: http://windows.microsoft.com

To backup and restore in the Windows7 operating system:

- Click **Start** → **Control Panel** → **Backup and Restore** → **Set up Backup** to start a backup program.
- Select the drive to save the backup and click **Next**.

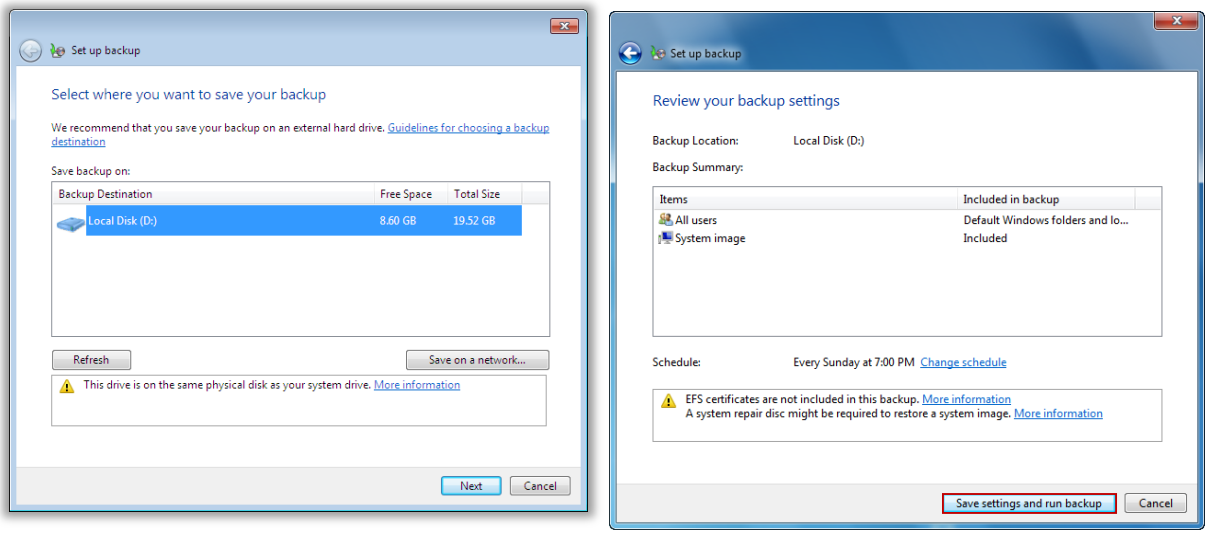

Figure 05-01: Screenshot of Backup and Restore Window

- In the **What do you want to back up?** screen, check the option **Let Windows choose** and click **Next**.

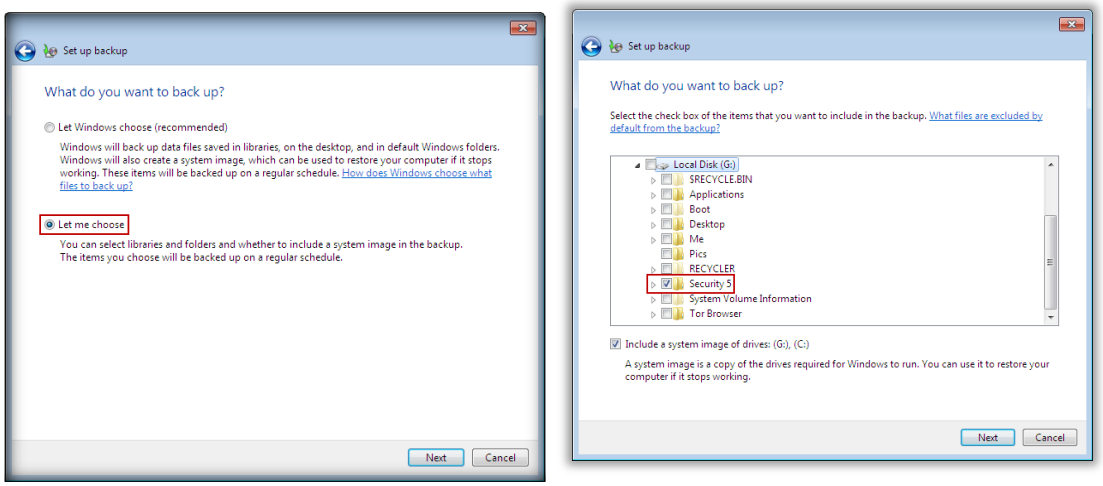

Figure 05-02: Screenshots of Set Up Backup Window

- **Backup in progress** appears, which completes the backup process.

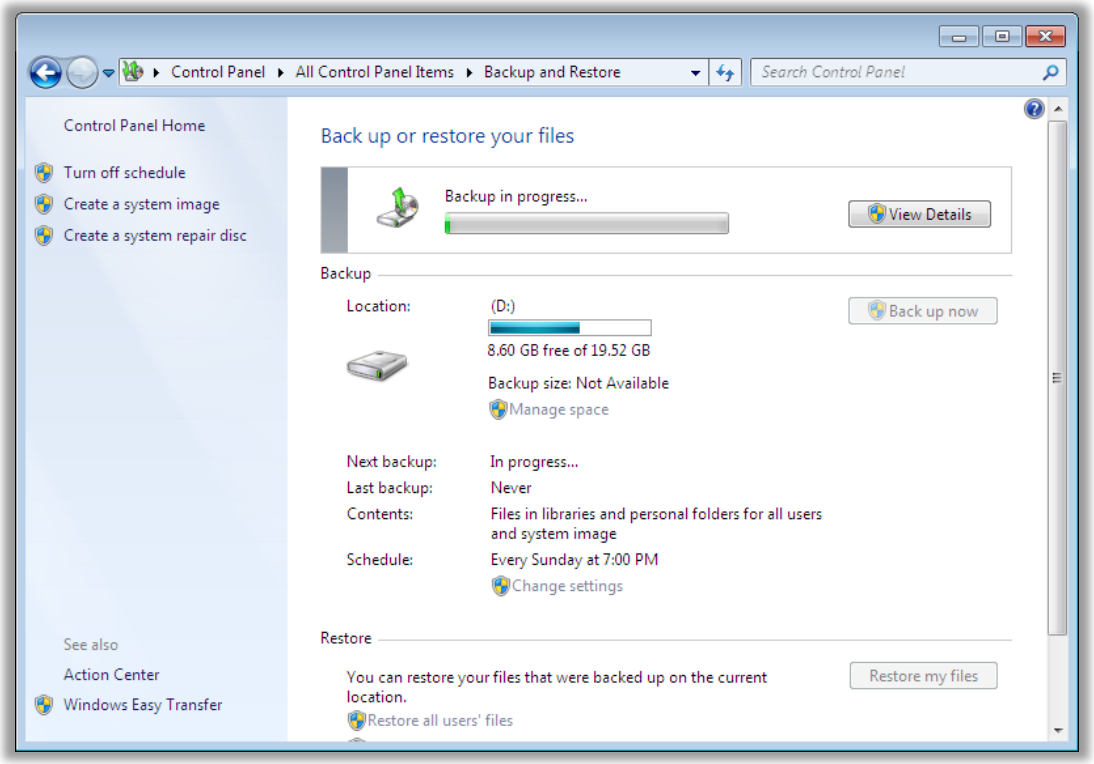

Figure 05-03: Screenshot of Backup and Restore Window

Restoring Data

Source: http://windows.microsoft.com

To backup and restore in the Windows7 operating system:

- Go to **Control Panel → Backup and Restore → Restore my files.**
- In the **Browse or search your backup for files and folders to restore** screen, click **Browse for folders** to restore a folder, and then click **Next.**
- In the **Where do you want to restore your file?** screen, check **In the original location** or **In the following location** to browse the desired location, and then click **Restore.**
- In the **your files have been restored** screen, click **Finish** to complete the restoration process.

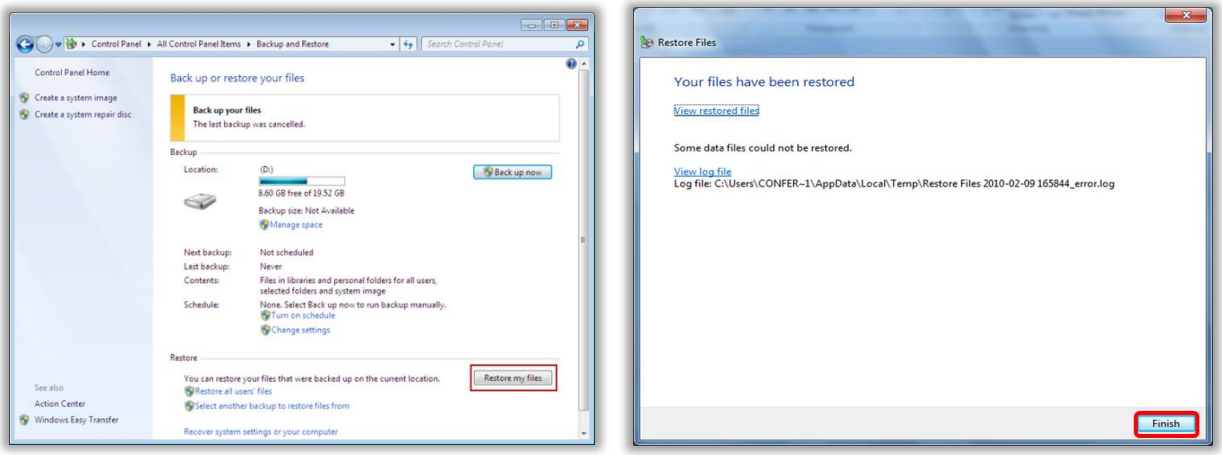

Figure 05-04: Screenshot of Backup and Restore Window

Securing Backup on Storage Devices with Encryption

Although making backups on the external storage media is safe and reliable, the external media may still be **stolen** or **corrupted**, making it impossible to restore the data. If it is stolen, the backup files may fall into the wrong hands.

The data that is backed up into the storage devices therefore should be **encrypted** with encrypting software. This makes the data present in the storage device unusable for anyone not **authorized to use** the device.

Some of the storage devices come with encryption software. Users may use this software to encrypt the backed up data, but often, this encryption software is clumsy and may not be reliable. Users may therefore choose to use any **third-party encryption software** such as TrueCrypt, or other software to encrypt backup data.

Time Machine (Apple Software)

Time Machine is a backup utility developed by Apple. It automatically saves up-to-date copies of everything on the Mac—photos, music, videos, documents, applications, and settings. If necessary, a user can go back in time to recover the data. Time Machine works with Mac and an external hard drive. Just connect the drive and assign it to Time Machine. It automatically backs up the entire Mac, including system files, applications, accounts, preferences, music, photos, movies, and documents. What makes it different from other backup applications is that, in addition to keeping a spare copy of every file, it remembers how the system looked on a given day. To launch Time Machine**,** navigate to the **System Preferences** window and click the **Time Machine** icon.

Features of Time Machine include:

- A user can browse for files using Cover Flow.

- A user can perform a **Spotlight** search to find what he/she needs across all backups.
- Before recovering a file, use **Quick Look** to verify the contents of the file, then click **Restore** to bring it back to the present.

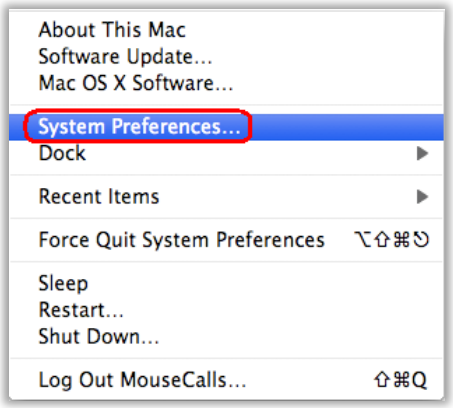

Figure 05-05: Selecting System Preferences

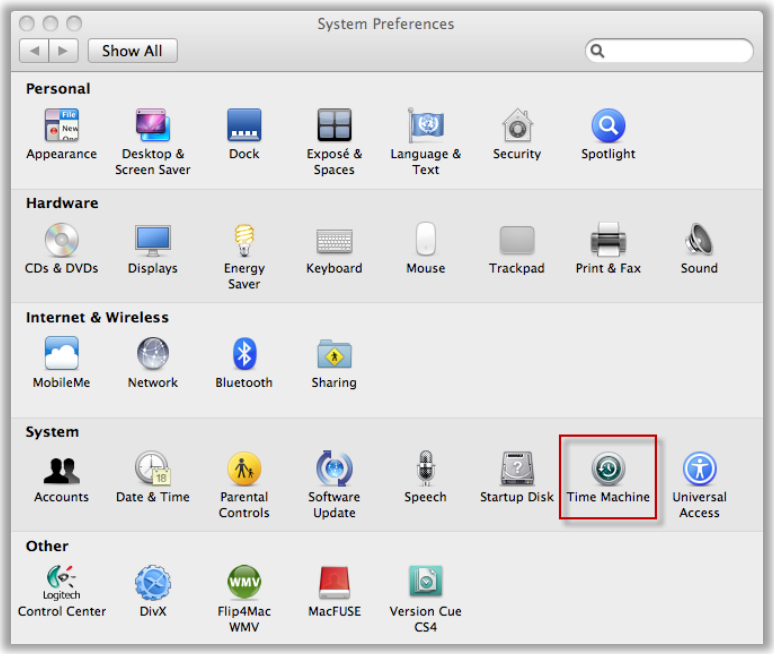

Figure 05-06: Selecting Time Machine

Setting Up Time Machine

The user can change the setting in the time machine according to his/her preferences by following these steps:

- Time Machine asks the user when a hard drive is connected to the computer for the first time to use it as a backup drive.

- Click **Use as a Backup Disk** to open the **Preferences** window to configure the disk as a backup disk.

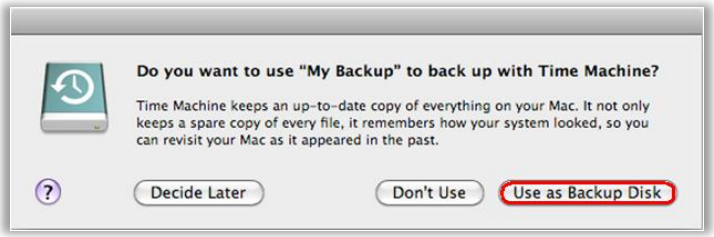

Figure 05-07: Selecting Use as Backup Disk

- In the **Time Machine preferences** window, check **Show Time Machine status in the menu bar** to see the status of backup.
- Click lock icon to secure the data present in the backup.

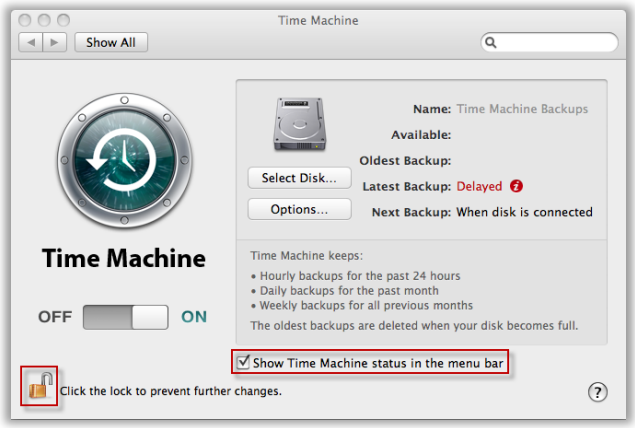

Figure 05-08: Selecting Show Time Machine status in the menu bar

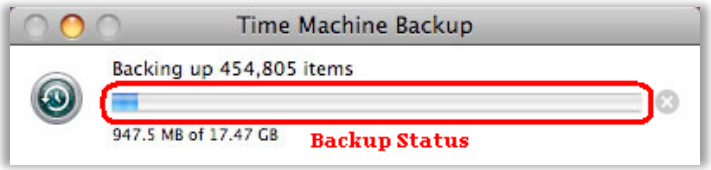

Figure 05-09: Time Machine Backup Status Window

Restoring Files from Time Machine Backups

To restore files from Time Machine backups:

- Connect the backup disk.
- Click the **Time Machine** icon in the dock.
- Use the timeline on the right side of the window to browse and backup files of a certain date and time.

- Select the file/folder and click the **Restore** button.

Figure 05-10: Restoring Files from Time Machine Backups

Windows Data Backup Tool: Acronis True Image Home 2011

Source: http://www.acronis.com

Acronis True Image Home 2011 provides home users with reliable and timeless backup and recovery of their home PC's operating system, applications, settings, and personal files. It automatically creates incremental backups once every five minutes allowing users to roll back their system, files, and folders to any point in time. It has online storage services to automatically back up valuable data or files over the Internet to a secure location

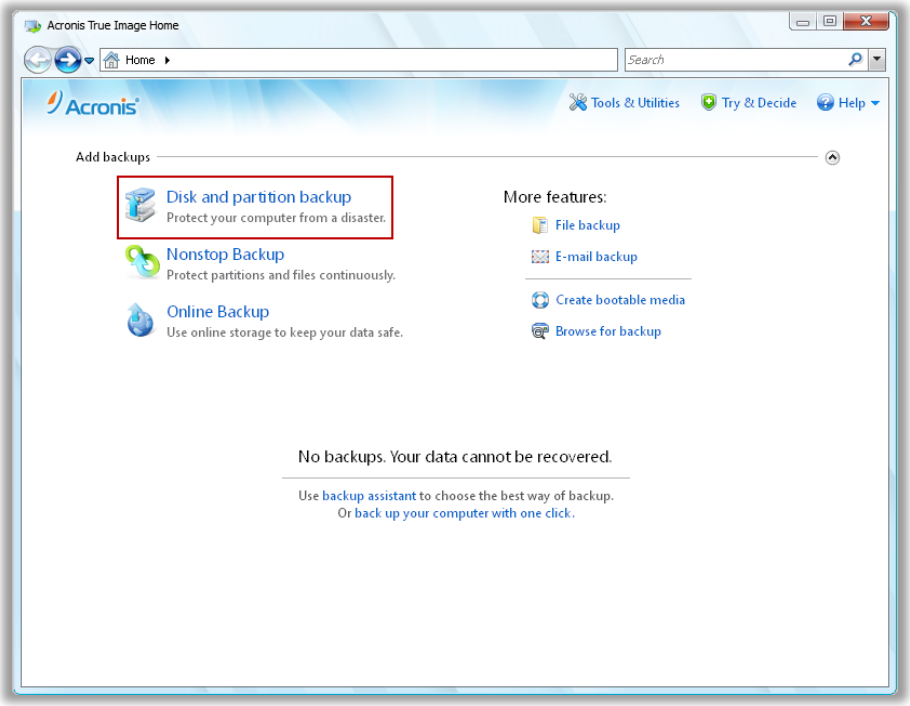

Figure 05-11: Adding Backups in Acronis

Windows Data Backup Tool: NovaBACKUP Home Protection

Source: http://www.novastor.com

NovaBACKUP Home Protection automatically backs up and protects important files on all of your computers from one easy to use control panel

Features:

- Automatic processes continually update your protection—no need to remember to run backups.
- Central management makes it easy to stay on top of all of the data in your home.
- Disaster recovery and full disk imaging options allow you to restore your entire system.
- Fast bit technology updates your backups with bit-level incremental changes.

Figure 05-12: Refreshing Backup in NovaBACKUP Home Protection Tool

Data Backup Tools for Windows

Genie Backup Manager Home

Source: http://www.genie9.com

Genie Backup Manager Home backs up your photos, media, email, and personal files and folders in a secure location and recovers your data in an instant. It performs a complete backup of your system (disaster recovery) or simply backs up only your personal data.

Norton Ghost

Source: http://www.symantec.com

Norton Ghost safeguards your system, settings, applications, and files with flexible, comprehensive backup protection and recovers your system and data when there are system failures. It saves recovery points to an FTP site for easier off-site management and even backs up your data to network-attached storage devices.

R-Drive Image

Source: http://www.drive-image.com

R-Drive Image is a utility providing disk image files creation for backup or duplication purposes. A disk image file contains the exact, byte-by-byte copy of a hard drive, partition or logical disk and can be created with various compression levels on the fly without stopping Windows OS and therefore without interrupting your business. These drive image files can then be stored in a variety of places, including various removable media such as CD-R (W)/DVD, Iomega Zip or Jazz disks, etc.

TurboBackup

Source: http://www.filestream.com

TurboBackup is used to back up work, synchronizing between laptop, netbook, or desktop PCs; scheduling unattended after-hours backup; exporting data to off-site locations to prepare for disaster recovery; or archiving personal data to a CD/DVD or memory stick for sharing or storage.

NTI Backup Now

Source: http://www.ntibackupnow.com

NTI Backup Now is a backup and restoring solution for SMB MIS, LAN, SOHO, personal desktops, notebooks, and netbooks. It allows you to back up your complete PC system or specific files and folders that includes your data, applications, photos, videos, music, financial documents, and settings.

PowerBackup

Source: http://www.cyberlink.com

PowerBackup offers three backup methods: full, differential, and incremental to perfectly suit user needs. Full is a complete backup of all files. Differential mode archives changed or new files. Incremental mode archives new files created since the last backup.

Backup4all

Source: http://www.backup4all.com

Backup4all is a backup program for Windows that protects your data from partial or total loss. It automates the backup process to save you time, compresses the data to save storage space (using standard zip format), and optionally encrypts data to protect it from unauthorized usage.

BounceBack Ultimate

Source: http://www.cmsproducts.com

BounceBack automatically backs up files that have been changed or newly created on a continuous basis. It backs up drive contents and restores single files or folders quickly and easily.

OopsBackup

Source: http://www.altaro.com

With Oops!Backup you can rest assured that your data is protected every time you make a change - without slowing down your PC. It Detects file changes automatically and versions and backs up the files for you.

MAC OS X Data Backup Tool: Data Backup

Source: http://www.prosofteng.com

Data Backup is a utility that allows you to back up, restore, and synchronize your valuable data with minimal effort.

Features:

- Allows you to back up your iTunes or iPhoto files as well as other important data or your entire system
- Schedules your backups to run automatically at a specific time
- Backs up to any mounted drive including FireWire, USB, ATA, or networked drives
- Creates an exact copy of a folder or drive, including bootable OS X backups
- Automatically runs any data backup task on specific days or other recurring basis

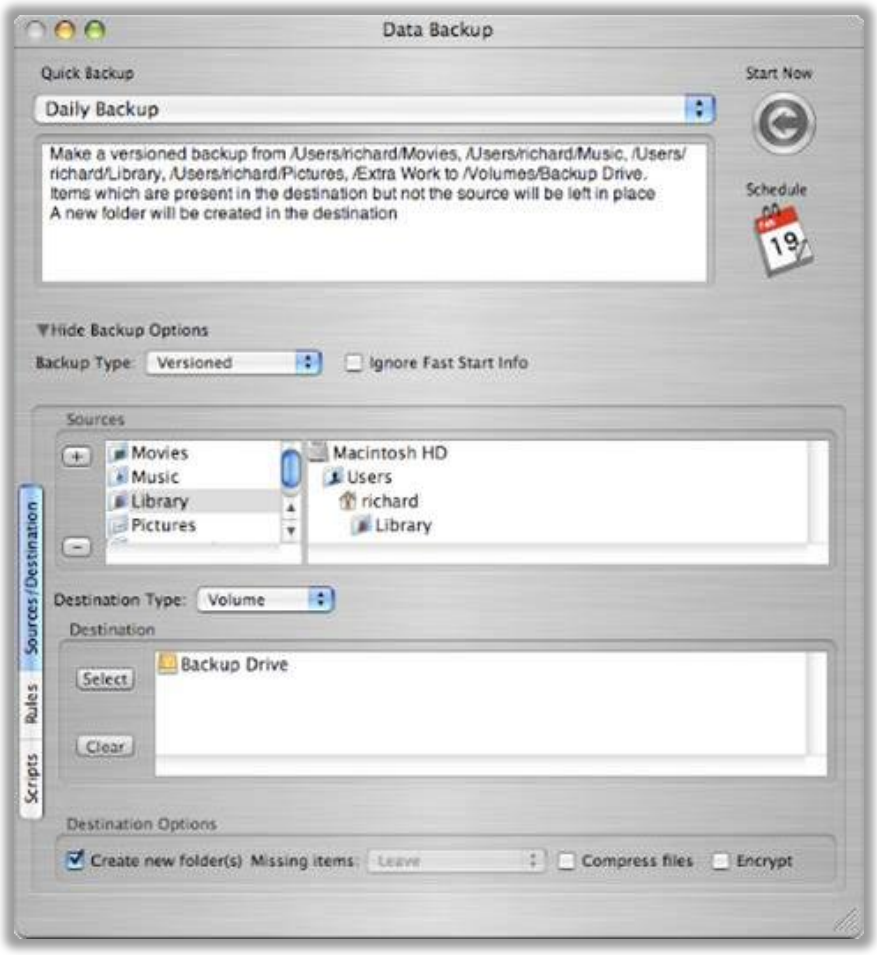

Figure 05-13: Selecting Data to Back Up in Data Backup Tool

MAC OS X Data Backup Tool: SmartBackup

Source: http://freeridecoding.com

SmartBackup is a backup utility that creates fast and efficient backups of your data, or a full bootable clone of your system. It can back up to anything that is mountable on your Desktop as well as external hard disks, flash drives, iPods, and any kind of network shares.

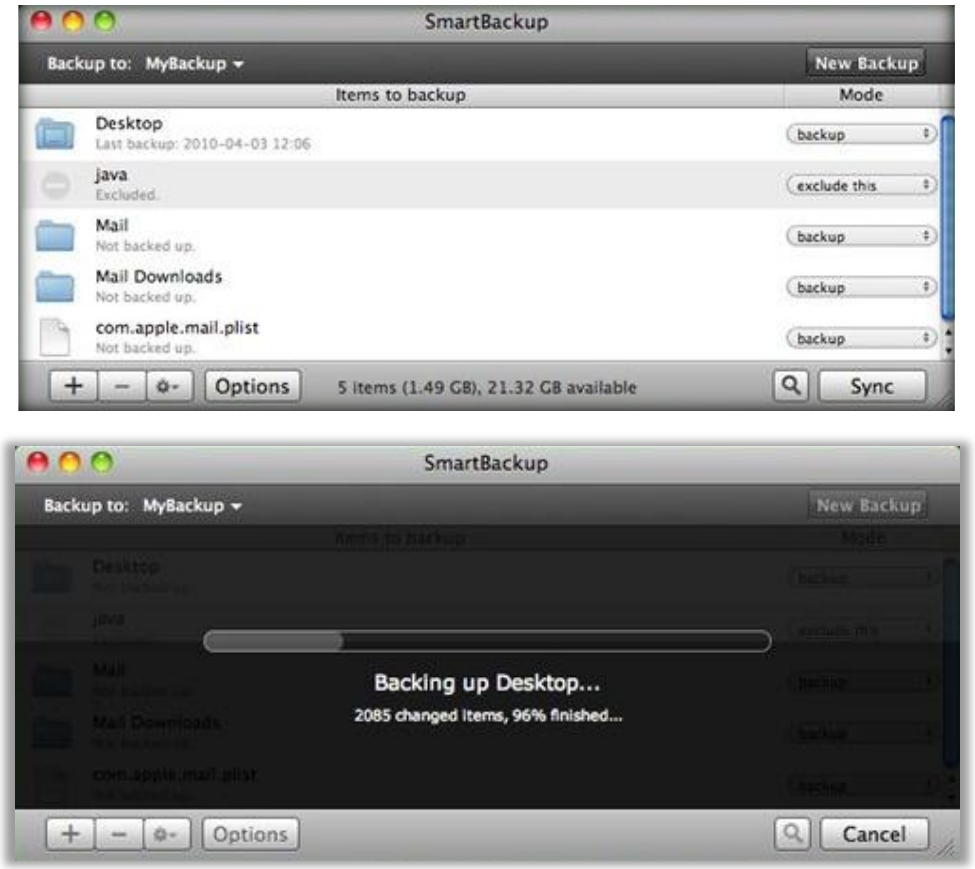

Figure 05-14: Selecting Items to Back Up in SmartBackup Tool.

Data Backup Tools for MAC OS X

Synchronize! Pro X

Source: http://www.qdea.com

Synchronize! Pro X is a professional-strength file synchronization and backup utility for Mac OS X.

iBackup

Source: http://www.grapefruit.ch

iBackup backs up the data, system, and application settings of a user. It backs up system settings (e.g., system preferences, mail, iPhoto, iTunes, and third-party applications settings).

Roxio Retrospect

Source: http://www.retrospect.com

Roxio Retrospect provides individuals with the reliability, ease of use, power, and flexibility they need to protect critical data on their Macs. Features include remote management of one or more backup servers and disk-to-disk-to-tape backups.

SuperDuper

Source: http://www.shirt-pocket.com

SuperDuper produces fully bootable backups of the newest version of OS X. It allows you to copy your Time Machine backups to other disks.

Tri-BACKUP

Source: http://www.tri-edre.com

Tri-BACKUP backs up your files and disks, preserves each successive version of your documents, and automatically runs your backup.

MimMac

Source: http://www.ascendantsoft.com

MimMac is a backup and cloning utility, designed to back up, synchronize, merge, and clone data.

Windows Data Recovery Tool: Recover My Files

Source: http://www.recovermyfiles.com

Recover My Files data recovery software recovers deleted files emptied from the Windows Recycle Bin, or lost due to the format or corruption of a hard drive, virus, or Trojan infection or unexpected system shutdown or software failure.

Features:

- File recovery after accidental format, even if you have reinstalled Windows
- Disk recovery after a hard disk crash
- Retrieves files after a partitioning error
- Retrieves data from RAW hard drives
- Recovers documents, photos, videos, music, and email
- Recovers from hard drive, camera card, USB, zip, floppy disk, or other media

Figure 05-15: Recover My Files Tool Screenshot

Windows Data Recovery Tool: EASEUS Data Recovery Wizard

Source: http://www.easeus.com

EASEUS Data Recovery Wizard provides a comprehensive data recovery solution for computer users to recover lost data due to partition loss or damage, software crash, virus infection, and unexpected shutdown.

Features:

- Recovers deleted or lost files emptied from the Recycle Bin
- File recovery after accidental format, even if Windows has been reinstalled
- Disk recovery after a hard disk crash
- Retrieves data from RAW hard drives
- Recovers office document, photo, image, video, music, email, etc.
- Recovers data from a hard drive, USB drive, memory card, memory stick, camera card, zip, floppy disk, or other storage media

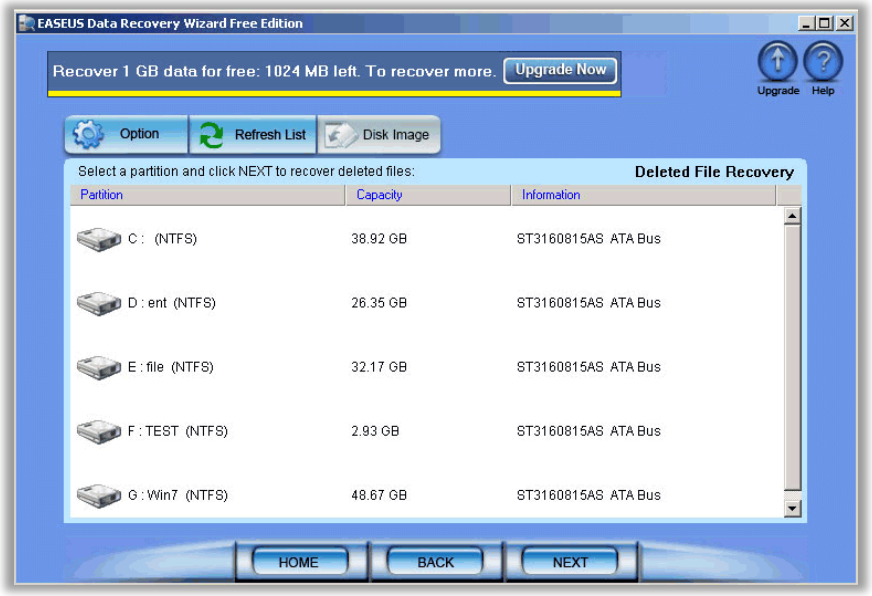

Figure 05-16: Selecting a Partition to Recover Deleted Files in EASEUS Data Recovery Wizard

Data Recovery Tools for Windows

Advanced Disk Recovery

Source: http://www.systweak.com

Advanced Disk Recovery scans the entire system for deleted files and folders and allows the user to recover them. Hard drives, partitions, external devices, and even CDs and DVDs can be scanned for recoverable files using Advanced Disk Recovery.

Handy Recovery

Source: http://www.handyrecovery.com

Handy Recovery is data recovery software designed to restore files accidentally deleted from hard disks and memory cards. The program can recover files damaged by virus attacks, power failures, and software faults or files from deleted and formatted partitions.

R-Studio

Source: http://www.data-recovery-software.net

R-Studio is a data recovery solution to recover files from FAT12/16/32/exFAT, NTFS, and NTFS5 (created or updated by Windows 2000/XP/2003/Vista/2008/Win7). It functions on local and network disks, even if such partitions are formatted, damaged, or deleted.

VirtualLab Data Recovery

Source: http://www.binarybiz.com

Regardless of the reason for data loss, accidental format, damaged partition, virus attack, deleted files, even a formatted hard drive, VirtualLab Data Recovery software does the job! VirtualLab is incredibly easy to use, yet so powerful and robust that it is used daily by data recovery companies world-wide.

File Scavenger

Source: http://www.quetek.com

File Scavenger is a file "undelete" and data recovery utility for Windows. It can recover files that have been accidentally deleted (including files removed from the Recycle Bin, in a DOS window, from a network drive, from Windows Explorer with the SHIFT key held down) provided that recovery is attempted before the files are permanently overwritten by new data.

Windows Data Recovery Software

Source: http://www.diskdoctors.net

Windows Data Recovery Software can recover data from any logical crash or cause for data loss on Windows. It combines TurboScan and File Tracer technology to recover data from even the most severely corrupted hard drives.

MAC OS X Data Recovery Tool: Boomerang Data Recovery Software

Source: http://www.boomdrs.com

Boomerang Data Recovery Software for MacOS X recovers accidently deleted files, folder, document, lost or damaged partitions, RAID volumes, camera/flash cards, etc.

Features:

- Recovers a complete disk that no longer mounts or is formatted
- Re-assembles RAID volumes and helps recover mission critical data
- Scans the entire disk and recovers deleted files and documents

Figure 05-17: Performing Drive/Disk Recovery in Boomerang Data Recovery Software Tool

MAC OS X Data Recovery Tool: VirtualLab

Source: http://www.binarybiz.com

VirtualLab is non-destructive data recovery software that recovers deleted files, damaged or missing volumes, formatted disks, iPods, and even photos. It performs an exhaustive scan of the drive to locate lost partitions and files.

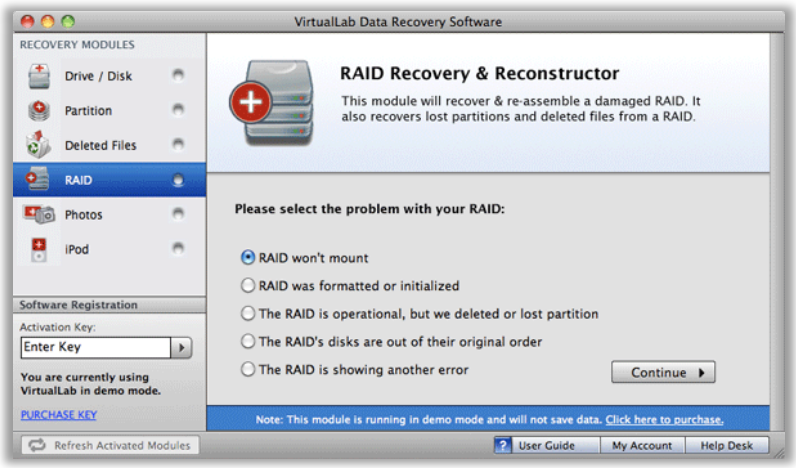

Figure 05-18: Performing RAID Recovery and Reconstructor in VirtualLab Tool

Data Recovery Tools for MAC OS X

DiskWarrior

Source: http://alsoft.com

DiskWarrior is a utility to eliminate directory damage and recover your files, folders, documents, and data from a failing hard drive.

AppleXsoft File Recovery for Mac

Source: http://www.applexsoft.com

AppleXsoft File Recovery for Mac is a data recovery software tool that recovers Mac data from corrupted, deleted, or formatted partitions and from crashed drives where Macintosh-based file system are installed.

Disk Doctors Mac Data Recovery

Source: http://www.diskdoctors.net

Disk Doctors Mac Data Recovery software recovers lost and deleted data from HFS+ and HFSX file systems on Mac OS X.

R-Studio for Mac

Source: http://www.r-tt.com

R-Studio for Mac is specially designed for a Mac OS environment and recovers files from HFS/HFS+ partitions. It also recovers data on disks, even if their partitions are formatted, damaged, or deleted. Flexible parameter settings give you absolute control over data recovery.

Data Rescue

Source: http://www.prosofteng.com

Data Rescue recovers files from a problem hard drive or that have been previously deleted.

Stellar Phoenix Mac Data Recovery

Source: http://www.stellarinfo.com

Stellar Phoenix Mac Data Recovery recovers data lost or deleted from HFS, HFS+, WFS Wrapper, FAT file system volumes, and data from HDD, USB flash drives, memory cards, and iPods.

FileSalvage

Source: http://subrosasoft.com

FileSalvage is a Mac application for exploring and recovering deleted files from a drive or volume. It is designed to restore files that have been accidentally deleted, become unreadable due to media faults, and stored on a drive before it was re-initialized/formatted.

TechTool Pro

Source: http://www.micromat.com

TechTool Pro is a full-featured utility program that contains options for testing and repair, maintenance (including disk defragmentation), and data recovery for Macintosh OS.

Physical Security

Physical security is the **protection** of **hardware**, **personnel**, **data**, and **networks** from attacks that cause **loss** or **damage**. Factors affecting physical security include natural disasters, fire, theft, vandalism, terrorism, and burglary.

Physical security is necessary to:

- Prevent any unauthorized access to the computer systems
- Prevent tampering /stealing of data from the computer systems
- Protect the integrity of the data stored in the computer
- Prevent the loss of data/damage to systems against any natural calamities

Critical components to physical security include multiple **locks**, fireproof safes, fencing, walls, water sprinklers, surveillance and notification systems, heat sensors, smoke detectors, and intrusion detectors.

Physical Security Measures: Locks

Physical security of the information systems is a **major concern** as the theft of data and information systems has become common. Keys and locks are one of the **safeguards** for securing critical information. Although keys and locks may not greatly help the physical security, they act as the **primary method** of **controlling physical access** to the information, information systems, and removable storage devices. Locks may be used to:

- Protect the computer from unauthorized access by locking the doors and windows in the computer premises
- Lock the CPU and monitor to prevent them from being stolen

PCs include a locking feature. There is usually a socket on the front or a dongle at the back that can be used to lock the PC with a sturdy cable. CPUs, laptops, and notebooks can also be secured by locks.

Figure 05-19: InnerLock System for CPU

Figure 05-20: Monitor Security Cable C1

Physical Security Measures: Biometrics

Biometrics consists of methods to recognize individuals from their **physical** or **behavioral traits**. No two individuals possess the same physical traits such as fingerprints, eyes, face, etc. These traits can be used to authorize only certain people to access the hardware.

Types of biometric security authentications include:

- **Fingerprinting:**

  The fingerprinting recognition mechanism involves identifying the unique fingerprint of an individual.

- **Retina scanning:**

  The retina recognition mechanism involves identifying the unique patterns of the retina by using a low-intensity light source.

- **Iris scanning:**

  The iris recognition mechanism involves identifying the iris of the eye, which is the colored area, with a video-based image acquisition system. The pattern of the iris is unique to every individual.

- **Voice recognition:**

  The voice recognition mechanism involves identifying the voice of an individual by identifying the unique speech characteristics such as the frequency between phonetics.

- **Face recognition:**

  The face recognition mechanism involves identifying the user by analyzing the distinctive features of the face such as the shape, pattern, and position of the facial features.

- **Vein structure:**

  Vein structure can also be used as a biometric trait to authenticate a person; the arrangement, location, and thickness of veins are considered unique biological traits and are compared with stored data, thus authenticating a person if there is a match.

Physical Security Measures: Fire Prevention

Fire is one element that can cause natural disasters. It may occur due to human error or because of hardware failures. To prevent it, users should remember that fire can break anywhere at any time. It needs three elements to break—fuel, oxygen, and an ignition. Fire accidents can bring heavy losses and destructions in the workplace and may cause major body injuries.

Fire preventive measures

To avoid fire-based accidents:

- Make sure all the emergency doors and corridors are kept clear.
- Use good quality wiring, tools, and equipment.
- Avoid using equipment that gives mild electrical shock.
- Keep the workplace dust-free and remove all the scraps as soon as possible.
- Ensure that the trash is emptied regularly.
- Install a fire alarm.
- Turn off all equipment after use.
- Prepare and implement a fire safety plan.
- Know how to use a fire extinguisher.

Physical Security Measures: HVAC Considerations

HVAC (Heating, Ventilating, and Air Conditioning) is the technology developed for the indoor **environmental comfort** of organizations. HVAC considerations include:

- Power supplies to a building should have overload protection to protect the equipment.
- Fuses and circuit breakers have to be used to prevent electric fire.
- Power stabilizers are recommended to avoid power fluctuations.
- HVAC is also referred to as climate control.

Securing Laptops from Theft

Portability plays a dominant role in the popularity of the laptops. Laptop clientele includes individuals who travel a lot—both business people and students. Laptop theft, however, has been a major security concern for laptop users. Stolen laptops account for **more than 20%** of the total security incidents that occur annually. Moreover, users **lose millions of dollars** due to the theft of laptops and the information stored in them.

Laptops have made computing a lot more personal, and users tend to **store confidential information** on them including bank account information, email account information, and personal information such as photos, videos, and emails. Users should follow the following measures to avoid laptops from being stolen and to recover them in case of a theft:

Do's:

- Note the laptop serial number and keep it safe.
- Choose a laptop skin in order to recognize it easily.
- Report laptop theft immediately.

Don'ts:

- Do not leave the laptop unattended (in the car or out in the office/home).
- Do not forget the password and avoid sharing it with others.

Laptop Theft Countermeasures

A lack of security measures allows an attacker to access the information stored on a laptop. The following countermeasures help users prevent and counter laptop theft:

- **Encrypt** sensitive data.
- **Back up** everything on the laptop.
- Install **tracking tools** on the laptop that help trace the location of the stolen laptop.
- Set **BIOS's password** on the laptop.
- Consider the laptop's PC **insurance**.
- Add third-party **privacy protection** for sensitive data.
- Use physical **locks**.
- Use strong, hardware-based security.

Module Summary

Backup is required in situations such as hardware failure, theft, system crash, and at the time of disaster.

Users need to back up whenever there are changes to important files, so that the latest copy is available even if the original is lost or damaged.

Online backup or remote backup is the method of off-site data storage in which the contents of a hard drive are regularly backed up to another computer or the Internet (remote server)

Normal, incremental, differential, and copy are the types of backups in Windows.

Physical security involves the protection of assets such as hardware, networks, and data from attacks that cause loss or damage.

Laptop theft leads to the disclosure of information such as usernames, passwords, confidential data, and other networking details related to connecting the laptop to the corporate or Internet environment.

Data Backup Checklist

- ☐ Back up important documents, photos, favorites, email, etc. to CD, DVD, tape or another disk at regular intervals
- ☐ Keep backup data in a safe place
- ☐ Keep multiple backup copies of important data
- ☐ Use encryption techniques to protect backup data
- ☐ Check for automated backup and scheduling features when selecting a backup tool or service as manual backups are vulnerable to human error
- ☐ If you are using an online data backup and recovery service, check service provider's stability and track record
- ☐ Continuously verify your backup process for its effectiveness

Physical Security Checklist

- ☐ Survey the building and deal with obvious problems
- ☐ Use strong locks for the doors and windows
- ☐ Install appropriate air-conditioning and fire-detection systems in special rooms
- ☐ Maintain a temperature of less than 30 degrees centigrade and a humidity between 20 and 80 percent in the computer room
- ☐ Maintain a backup of sensitive information and keep it in a safe place
- ☐ Minimize the amount of paper and sensitive information left on desks
- ☐ Lock the documents in cabinets

This page is intentionally left blank.