Small Business Backup/Disaster-Recovery Plan

Protect your data from viruses, deletion, and other disasters

Purpose

When you go into your office tomorrow, how long can you work before you'll need to use your computer.

How long before you need to send or receive an email?

How long before you need to check on an order or invoice?

How long before you need to record a sale and run a credit card charge?

But, what if your computers were stolen, destroyed in a disaster, or infected with a virus?

Just like seatbelts, fire extinguishers, and insurance, you need to prepare for data loss ***before*** it happens.

This guide will show how to setup a two-layer disaster-recovery plan to protect your company's critical data.

After you follow these steps, you will be able to quickly get back in business after a fire, flood, disk drive crash, virus - or any other problem that could wipe out your company's data.

Preparation

You'll need to store files and backup disk drives away from your office. It won't do you any good if your backup instructions are on a computer that was destroyed, or if your backup disk drives are also burned-up, flooded, or stolen.

Physical Storage

Rent a safe deposit box that is not extremely close to your office. If there is a flood or fire, you don't want to also lose your backups, because they were stored in the building next to your office.

The box needs to be large enough to hold a backup disk drive for each computer, along with printed copies of your recovery documents and any installation disks.

You won't need to access the safe deposit box very often - probably once every three to six months.

Digital Storage

Store large files on a file hosting service, such as:

- OneDrive: https://onedrive.live.com
- Dropbox: https://www.dropbox.com
- Google Drive: https://www.google.com/drive/
- Apple iCloud: https://www.apple.com/icloud/

For small files, email them to your personal (home) email address and/or store them in the same file hosting service you use for the large files.

NOTE: Do not store unencrypted passwords in these documents. If you need a secure way to store passwords, use a service like 1Password (https://1password.com/) or LastPass (https://www.lastpass.com/).

Step 1: Inventory your hardware and software

First, create an inventory of your computers and computer-related equipment.

You'll use this list to:

1. Select the right backup equipment, software, and service for your needs
2. Buy replacement equipment, if needed
3. File a police report, in case of equipment theft

Computer Hardware Inventory

Create a spreadsheet or word processing document. For each computer, record the following information:

- Name
- Brand and model number
- Serial number
- Operating System (and version)
- Hard disks
    - Internal or external
    - Total disk size
    - Amount of used disk space
- Processor
- Memory (RAM)
- Graphics card
- Any other cards installed

Include similar information for your other computer equipment, such as monitors, printers, network routers, cable modems, etc.

Software Inventory

If you follow this complete plan, you should not need to re-install software. The recovery steps will automatically have the programs installed. However, it's best to be prepared to re-install programs on replacements computers.

Create a word processing document to hold the installation instructions for your software. For each program, record:

- Name of the program
- Your customer account name/number
- License key
- Installation instructions
- URL to downloadable installation file

For downloaded installation files - programs that don't have an installation disk - copy them to the file hosting service you selected for "Digital Storage", in the "Preparation" section.

Print your inventory document and installation instructions. Store them and any installation disks/CDs/DVDs in your safe deposit box.

Step 2: Protect your computers from disasters

The best way to recover from a disaster is to prevent it from happening in the first place.

Protection from Electrical Problems

There are two electrical problems to protect yourself from: electrical damage from a power surge and losing un-saved data during a power outage.

For your computers, choose a battery backup that will give you at least 15 minutes of power for your computer and monitors - so you can safely save your work and shut them down.

Some battery backup devices have some outlets that only have surge protection - they are not connected to the battery.

Make sure you plug your computer and monitor into an outlet with both surge protection and battery power. If you plug the monitor into an outlet without battery power, you won't be able to see what you're doing when you try to shut down the computer safely.

Also, get a surge protector for your internet modem.

I've personally experienced a lightning strike at my building. My computers were protected. However, I didn't have a surge protector on the cable modem - which shorted out. You may not need a battery backup for your internet modem, but a $20 surge protector can save you from losing internet access, as you rush out to buy a replacement modem.

Recommended battery backup brands: APC, CyberPower, and Tripp Lite.

Automated Updates

Unfortunately, we live in a world where computer viruses are a dangerous reality. To reduce the chance of a virus infecting your computers, turn on automatic updates for your operating system and anti-virus software.

If you don't have anti-virus software installed on your computers, this is the time to do that. After installing, run a virus check, to see if any computers are infected.

Recommended anti-virus vendors: Bitdefender, Kaspersky, and Webroot. I do not recommend Symantec, due to negative performance experiences with it.

Most anti-virus vendors offer 30-day free trials. When you choose one that looks like it fits your needs, install the trial version on one or two computers. See how well it performs, before you buy it for every computer.

Sometimes, anti-virus programs try to protect your computers too much. They secure your computers to the point where they may prevent you from running your legitimate programs.

If this happens, you may need technical help to add your trusted programs to the anti-virus program's "exclusion" list - programs that should not be prevented from running.

Replace old disk drives

Disk drives eventually wear out. If you have computers that are 3-4 years old, you may want to replace their disk drives.

In the next step - creating disk "clones" - many of the cloning programs include the ability to copy your disk drive to a replacement disk drive.

NOTE: You may want help with this, from someone familiar with this type of disk replacement.

Step 3: Create "clones" of your computers

The first layer of this disaster-recovery plan is to make an exact duplicate of each computer's disks - a "clone", or "disk image".

If you need to replace a computer, you'll copy this clone onto the new computer. Then, the new computer will look exactly like the computer it's replacing.

The clone copies everything from the computer, including installed programs and their configurations. Because of this, you will not need to re-install any programs on the new computer.

To make a clone, you need a cloning/imaging program and an external USB disk drive that is larger than the amount of data stored on the computer's disk drive.

Cloning/Imaging Programs

You need a program to create the clones. I recommend these three.

They often have free (limited-feature) versions, or discounts when buying copies for multiple computers. For paid versions, expect to pay around $30 - 40 per computer.

- EaseUS Todo Backup: https://www.easeus.com/
- Paragon Backup & Recovery: https://www.paragon-software.com/#
- Acronis True Image: https://www.acronis.com/en-us/

External USB Drives

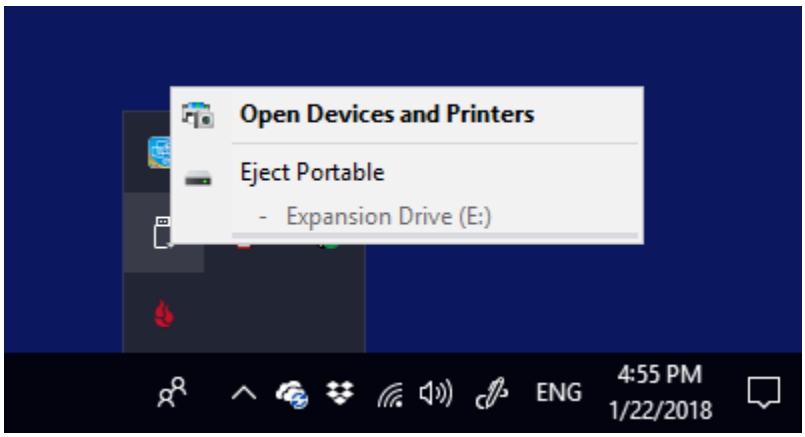
You will need an external USB drive for each computer.

A 1 Terabyte drive from Samsung, Seagate, Toshiba, or Western Digital (which is probably more space than you will need), costs around $55.

Creating the Disk Clones

Follow these steps to create your disk clones.

- Install the cloning software
- Label a USB drive with the computer name and plug it in to the computer
- Run the cloning program
    - This takes 30 to 60 minutes per computer, on average
- Safely detach the USB drive from the computer (see image below)
- Store all the USB drives in a safe deposit box
- Repeat this process every 3-6 months, to always have fairly-recent clones



Step 4: Remove unused files (optional)

With your disk drives backed up locally, it's time to prepare for the cloud-based backup.

The first time you run a cloud-based backup program, it needs to upload all the files from the computer. This can take several days - for each computer. You can reduce this time by first removing unused programs and files from your computers.

If you are uncomfortable deleting anything, you can skip this step. If you have any concerns, it's safest to leave the unused files on the computer.

To reduce the amount of data to upload:

- Uninstall unused programs
- Remove user profile data of former employees
- Run "Disk Cleanup"
    - Remove temporary files
    - Remove "System Restore Points"
    - Remove "Shadow Copies"

Step 5: Select the cloud-based backup service

Your disk clones are exact duplicates of your disks - at the time you make the clones. As you work, you create new files and change existing files. A cloud-based backup service will hold backup copies of the new/changed files.

When selecting a cloud-base backup service, you need to consider:

- Do you have any regulatory requirements for your data?
    - HIPAA compliance for medical data
    - PCI DSS for credit card information
    - Other standards for your industry
- Do you need to backup USB drives attached to your computers?
    - Some services do not allow this, or charge more for this.
- How much data do you need to back up?
    - Some services allow unlimited storage. Others charge by the amount of space used.
- Does your internet service have a data cap/limit?
    - Your initial backup may exceed this limit
        i. If so, consider a service where you can do the initial backup by mailing in disk drives - like Backblaze Fireball https://www.backblaze.com/b2/contact-fireball.html

Compare the costs of the services below, using your specific requirements.

Recommended cloud-based backup services

Backblaze: https://www.backblaze.com/business-backup.html

Carbonite: https://www.carbonite.com/backup-software/buy-carbonite-safe/

CrashPlan: https://www.crashplan.com/en-us/business/

iDrive: https://www.idrive.com/small-business

Mozy: http://mozy.com/product/mozy/business

Step 6: Setup the cloud-based backup software

After signing up for the service that best fits your needs, you can start installing the backup software on your computers.

Because the service can consume much of your internet traffic, you may want to install the backup software on one computer at a time. Start with the computer that stores the most important data first. When the first computer has finished, install the software on the computer with the next-most important data.

Cloud backup software settings

When you install the cloud backup software, you may want to change some of the default settings.

- Exclude files in these locations
    - Directories/folders for OneDrive, Google Drive, Dropbox, etc.
    - Network Attached Storage (NAS) devices, or "network shared drives"
        - These are files stored on one computer/device, but shared with other computers on the network
        - Exclude these drives from all computers **except** the one that holds the files.
- Set the hours to perform the backup
    - Cloud backup software uses a lot of your internet bandwidth. In order to not interfere with your company's normal internet use, you may want to schedule the backup software to only run outside of business hours.

Step 7: Prepare for recovery

Now that you have your two-layer backup plan in place, you need to plan what to do if you ever need to use it to recover your computers.

In your computer inventory, prioritize them by which ones you need to recover first.

It may take several hours to restore the latest files from the cloud-base backup service. It you replace all your computers and try to restore them all at the same time, it may be days before any one of the computers is fully-restored.

At first, only install the cloud-based backup software on the critical computers. Once their files have been restored from the cloud, install the cloud-based software on the non-critical computer and have them begin recovering their new/changed files.

While the critical computers are recovering their files from the cloud, you can start recovery of the non-critical computers with the cloned drives. Just don't install the cloud-based backup software, and start recovering the non-critical computers' files, until the critical computers have been fully-restored.

Need some help?

If you have a question about anything in this guide, or want help with setting up a disaster-recovery plan for your business, contact me (Scott) at:

Website: http://LillySoftwareConsulting.com/SBBDRP

Email: Scott.Lilly@LillySoftwareConsulting.com

Phone: 832-862-7414