# Introduction to Backing Up and Restoring Data


## Jennifer Vesperman

**jenn@linuxchix.org**


**2002-02-24**

### Revision History

Revision 0.1 2002-02-16 Revised by: MEG
Converted from text file. Modified wording.
Revision 0.2 2002-02-19 Revised by: MEG
Incorporated Jenn's changes.
Revision 0.3 2002-02-24 Revised by: MEG
Conforming to LDP standards.


This article provides an overview for backing up and restoring data, independent of operating system or system architecture. In this article, the author explores backup techniques as well as planning backups.


# 1. Introduction

## 1.1. Copyright Information



## 1.2. Overview

All the information you keep in your computer is stored on a hard drive. The important thing to know about hard drives is that they have moving parts - and like all things which move, those parts wear out eventually. So you need to keep a copy of your information on something else as well.

That's not the only reason to keep a copy somewhere else - your computer may be in a fire or a flood. A thief might steal the computer. Lightning might strike it. Someone might make a mistake and wipe out your database, without doing any damage to the computer itself.

So we store the data somewhere else as well. Not instead - most things you can back your information onto aren't any safer than the hard drive. But having it in two places is safer than one. Having it in three is even safer.

And then we store the backup (the second place) somewhere safe. Preferably in a different building - if it's in the same building and the building burns down or floods, you've lost both your original information and your copy.

# 2. Backup Media

There's a bewildering variety of things you can back up onto. There are floppy disks, tapes, removable hard disks, rewritable CD-ROMs - and by the time you read this, probably three or four other options. Here's the important thing: it doesn't matter which type you use.

It's a good idea to have something which you find easy to use. It's a good idea to have something big enough to put a single copy of all your information on one physical thing - one tape, or one CD-ROM. Two at most. But other than that, it doesn't matter which type you use. There's probably someone who understands computers who you trust, even if it's the staff in a particular specialist computer store. Take their advice.

Your backup media (the thing you back up on to) probably comes with software which will ask which files you want to back up, and will copy them onto the backup media for you. If not, ask your friendly specialist for help - there are too many ways to actually do a backup for me to write them all, and they'll change by the time you read it anyway. But in the following section, I'll give you some advice about what you might want to copy.

# 3. Backup Strategies

With as much data as is stored on a modern computer system, how do you decide what to backup? Should you just put the entire system on a CD or tape and be done with it? There are several problems with putting your entire system in a backup, not the least of which is cost of tapes and CDs. Also, the time to perform a backup is increased when the entire system is stored.

As long as you have the original CDs for your software, there is no need to include the programs themselves in backups. For example, your operating system and word processor shouldn't be backed up. The data files, however, cannot be recreated so you should include them in backups.

You DO want to backup:

- all your web pages, databases, and anything that you made or would have trouble replacing
- all the information from your financial software
- all the information from inventory control, customer databases, or other specialist business software
- important correspondence
- internal documents (important memos and the like)
- anything you would suffer for lack of if it lost

You MIGHT want to backup:

- your email, especially if it has customer queries, contact data, or other business-critical information
- preferences or bookmarks from web browsers
- your personal settings for how *your* computer works
- anything that would be a nuisance if it was lost

You probably DON'T need to backup:

- your operating system, so long as you have the original disks
- your software, so long as you have the original disks
- strictly temporary files (like a webcache, or anything in the trash can)
- anything that you are CERTAIN you won't need if the entire computer becomes rubbish.

How many days worth of information could you afford to lose if your computer crashed? What about if your office or home burned down? What about if most of your city was wiped out by a tornado or a flood?

The answers to these questions will tell you how often you should do a backup, and roughly where you should store them.

The computer crash one is for your most frequent backup - usually a daily backup, stored in your office or home.

The office-burned-down is for your next most frequent backup, usually a weekly backup stored in a secure place in another building - possibly a friend's place, or a friendly business whose backups you store. (Exchange backups each week.)

The final is often a monthly or six-monthly backup, and is stored somewhere distant - and in some cases, isn't done at all. It's a matter of choice, and what risks you want to take.

Any backup plan is simply a way of controlling risk. You risk losing a day's, a week's, a month's or a year's data - instead of risking losing it all. When devising your backup plan, think about how much risk you are willing to take.

# 4. Restoring

Always make sure you have a way to restore the information from your backup to the main system, that doesn't involve using the backup itself. If your restoration program is saved as part of your backup copy, you might not be able to restore your data in a crisis - because to do the restoration, you need the software that has to be restored! It becomes a 'catch-22' situation. Usually, having the installation disks for your backup program will prevent the 'catch-22'.

> **Note:** Always test the restoration process of your backup. If you have a spare computer, test restoring on that. Otherwise, test it on a separate folder on your main computer - make sure it doesn't overwrite your primary copy of your information!

In a perfect world, you test your restoration process by getting a blank computer, as if you'd lost your computer entirely and were starting from scratch. Install the operating system, your main programs, and your backup program from their original disks. (make sure those disks are still for sale! If your office or home burns down, your insurance company will be buying them for you - assuming you're insured.) Then restore your information from the backups, using the instructions given in the backup-program's manuals.

In the real world, do as much of that as you can. At minimum, restore the information from your backup tapes (or whatever) into an empty directory of your computer's hard drive. DO NOT overwrite your current information!

Be aware that you will probably need to use exactly the same backup program to restore your data as you used to save it. If that program becomes unavailable, you will need to check with your local computer-knowledgeable person whether you need to change programs, or to keep a copy at each of your backup-storage locations. If you do the second, make sure you won't need the backup-program just to install the backup program!

# 5. Related links

- Backup and Recovery at About.com (http://pcsupport.about.com/?once=true&)
- Linux Administration Made Easy, Backup & Restore Procedures (http://www.linuxdoc.org/LDP/lame/LAME/linux-admin-made-easy/backup-and-restore.html)