The Need for a Backup Strategy
by Kevin J. Vella
Uniblue Systems

So you’ve decided to backup your data but what is the next step? You must have a backup strategy irrespective of whether you are a home user or a business user. The depth of the strategy is the only variant between these two types of users.

As time goes by people and businesses are facing massive and ever-increasing amounts of data that are difficult to manage and that remain unprotected. In this light, the need for a backup strategy becomes critical. Let me just take email as an example: the 12/2004 issue of Smart Computing reports that 88% of adult PC users send and receive emails. The International Data Corporation reports that 16.8 trillion emails were transmitted in 2004 with this figure climbing to 19.7 trillion this year. According to Smart Computing, American businesses send about 9 billion emails a day. On average, home-users transmit around 435kb in email attachments every day. One other research firm estimates that typical corporations with 5000 employees accumulate 4 terabytes of emails every year. The size of my Outlook PST file for 2004 at work rested at 1.4Gb; at home it was 650Mb! And finally, Dataquest estimates that the total number of hard disk drives shipped in 2002 rests at 212.5m units representing around 8.5m terabytes of storage space.

Home-user data includes documents, audio and video files, scanned images, and digital photos. Businesses have marketing collateral developed and stored electronically, customer information stacked in databases, financial records posted in accounting packages, budgets and business plans recorded on network storage devices. As this list grows, the need for a backup strategy becomes even more obvious!

We usually advise customers to look at 5 key elements of any backup strategy:

1. **Invest in good Backup Software**: Read the reviews, visit the websites and look out for features and assurances that the product you are buying is reliable, fast and easy to use. Spend time reading the websites of the various suppliers. Some products cost no more than $40 but your data costs much more. Losing your data because the software you have bought is not effective means that you have thrown away an extra $40!

2. **Plan Your Backups**: Most software packages on the market have schedulers. Use these schedulers. It doesn’t take much time to set up a timetable for backups. Depending on how many times you use your PC you can schedule your periodical backups: at work, I backup every day at 9 a.m.. At home, I backup once a week.

3. **Check the Integrity of your Restore**: Even though you have backed up, what guarantee do you have that your data can be restored when disaster hits? The best way to ensure full “restorability” of your data is to buy a backup product that has bit-level verification (like WinBackup 2.0). Such a feature makes sure that while the product is performing your backup it checks all the data down to the level of bits and bytes. In essence, the software first backs up the data and then automatically performs a test restore to make sure that every single bit has been copied.

4. **Check the Integrity of your Backup Medium**: You can have the best software in the world and back your data every hour, however, if you do not have a good medium to store your archives, you are doomed. The second best way to ensure the restorability of your data is to choose good mediums and to do regular test restores from them.

5. **Check your hard drives regularly** and make sure you have good anti-spyware and antivirus software. There is no harm in checking hard drives for errors and bad sectors as these drives do fail over time.

Check out next week’s Newsletter: Coming Up: [Backup Features Part 1](#)