Is Your Data Safe?

Do you have a backup or disaster recovery plan in place to protect you in the event of data loss? Despite numerous threats to the safety of computer users data files constantly lurking about, very few back their data up on a regular basis, if at all.

A September 2008 study by Webroot Software Incorporated estimated that, “In 2007 alone, approximately 46 million people in the U.S. and UK lost personal files stored on their PCs.” The same study found that, “Two out of five PC users (43 percent) have lost digital files or data at some point in their lives” and, “One in five have lost files in the last two years alone.”

These are some pretty scary figures, but just as scary are the statistics on data backup practices. A national survey conducted by Bruskin Research for Iomega Corporation found that, “41 percent of computer users do not personally back up their data. More than two-thirds (69 percent) of home computer users and nearly half (46 percent) of work computer users personally back up their data only once a month or less often, or they never back up their data.”

There are many different causes of data loss, some more prevalent than others. Over the course of many years of data gathering and statistical analysis while practicing as a data recovery firm, engineers at Kroll Ontrack Incorporated have identified the leading causes of data loss. The top culprits

found are hardware or system problem/failure at 56%, human error at 26%, software corruption or program problem at 9%, computer viruses at 4%, and natural disasters 2%.

If you are currently backing up your critical data to an external medium of some sort on a regular basis, great; however, if you are backing up your data infrequently or not at all, then hopefully the aforementioned statistics will make a compelling case to proactively implement an effective back up plan. For starters, you want to make sure you know what and where all your critical data files are, and then back them up to a separate medium such as another hard drive, flash drive, optical disk, or a remote online back up server.

The recommended frequency of back ups varies from user to user depending on how often new critical data is added to the computer. In general, I recommend a weekly full back up at a minimum, preferably daily if critical files are being added or updated on a daily basis.

Unfortunately, even among those who do perform data back ups, many periodically forget to do them as planned. The antidote to forgetfulness is to utilize software that will run your scheduled back ups for you automatically. There are many software back up solutions available allowing a user to specify what files and folders they would like to back up, and then perform the back up task at specified time intervals. It’s a good idea to back up to a permanently connected device such as an external hard drive when using this method so that the storage medium will always be available when the scheduled time arrives.

While regularly backing up to an external device in your home or office is a huge positive step towards safeguarding your data, this method isn’t going to help you in the event of a natural disaster such as a fire or flood. To protect yourself from such unfortunate events, I recommend using an online remote back up solution. With an internet connection and a

subscription to one of many available online back up services, you can have your data automatically and regularly backed up to a safe, off-site location.

If you are unsure how to devise and implement a data back up plan for your computer or where to even begin, I can help. Don’t become another data loss statistic, make the decision to back up and safeguard your data today!

-Ted Eiler
www.tecs-onsite.com
800.993.TECS (8327)
tedeiler@tecs-onsite.com