

# Monthly Cyber Security Tips

# NEWSLETTER



**February 2010**

Volume 5, Issue 2

## Backing Up Your Files

**From the Desk of Mike Lettman – CISO/CSA, State of Wisconsin**

### How important is backing up your data and testing those backups?

According to Kabooza-2009 Global Survey, more than 80% of computer users surveyed do not back up their home PC regularly, and 50% do not back it up at all. Developing a backup and recovery plan for data residing on your computer is an important step every computer user and organization should take.

Loss of data can be devastating, especially if the information cannot be recovered or reproduced. Whether data is lost due to a physical disaster, virus, theft, or accidental deletion, the recovery of the data cannot be accomplished unless you have a plan in place. The need to back up important data to ensure its availability in the event of loss or theft cannot be overstated. Backup and recovery plans are essential not only for government and businesses but also for home users.

### What should you backup?

All critical files, as well as any information not easily replaceable should be backed up. This could include business records and financial data, pictures, media files, emails, address book and calendars, and any other information that has value to the individual or organization.

### How do you backup data at home?

- **Copy files to other storage media.** Copy selected files to storage media such as CDs or DVDs.
- **Use your computer's backup tools.** Most operating systems now provide backup software designed to make the process easier.
- **Backup data at regular intervals.** Evaluate the importance of your data and the frequency of change in the data to determine the necessary frequency with which the data should be backed up. If your computer crashed today due to a hardware failure or virus could you afford to lose the data on it?

- **Verify the data has been backed up.** Backup media needs to be reviewed periodically to determine if all of the data has been backed up accurately. Use the "backup log" provided by most backup applications. Generate a "backup report" that can quickly identify problems or skipped files. Be sure to review these logs periodically.
- **Store the backup media in a secure location.** It is recommended that two backups be maintained: one on-site and one off-site. Backup media should be stored in a physically secure location.
- **Verify the ability to restore.** It is a best practice to periodically test that your backup data can be restored if loss occurs.

### What media can be used for backups?

- **USB Flash drives**, sometimes called "thumb" drives, typically have limited storage and may not be practical for storing large amounts of data. However if you just have a small number of sensitive files this is an easy way to copy files from your computer to a backup drive.
- **CDs** offer less storage capacity than flash drives and can be slow in copying and retrieving files however they are inexpensive. They are useful for home users with limited amounts of data to back up on a low budget.
- **DVDs** provide much greater storage capacity than CDs and tend to be inexpensive as well. Like USB flash drives they have limited storage and may not be practical for storing large amounts of data.
- **External Hard drives** are very effective backup devices. They typically have large storage capacity, and allow for extremely rapid copying of files and recovery of stored files.
- **Tapes** are commonly used in government and businesses where large amounts of data need to be backed up on a regular basis.
- **Online backup services** offer varying levels of storage and recovery options that can be tailored based on needs. It should be noted that there is a risk of storing PII (Personally Identifiable Information) or sensitive information with a third party service. You should take extra steps to make sure this meets your business and security needs.

**Note:** Many organizations have formal processes to backing up systems and no action by the end user is required.

For more monthly cyber security newsletter tips visit: <http://itsecurity.wi.gov/>

### Additional Information:

- **MS-ISAC Guidelines for Backing Up Information – A Non-Technical Guide**  
<http://www.msisac.org/awareness/documents/Backing-Up-Information-Guide.pdf>
- **Microsoft backup procedures for various Operating Systems**  
<http://www.microsoft.com/protect/data/backup/about.aspx>
- **StaySafeOnline**  
<http://www.staysafeonline.org/content/backupyourfilesanddata>

\*\*\*\*\*  
*The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure*

*manner within their work environment. Organizations have permission--and in fact are encouraged--to brand and redistribute this newsletter in whole for educational, non-commercial purposes.*

***Brought to you by:***



<http://itsecurity.wi.gov/>



<http://www.privacy.wi.gov/>



[www.msiscac.org](http://www.msiscac.org)