



# Guidelines for Maintaining, Protecting and Securing a Small Office/Home Office (SOHO) PC System

David B. Leach

Independent Consultant

***Industrial Process Optimization***



# OUTLINE

## ■ Outline

- **Personal Guiding Philosophy**
- **Preventative Maintenance Steps**
- **Backup and Disaster Recovery Considerations**
- **System Security & Integrity Considerations**
- **Useful Third Party Software Utility Apps**
- **Internet Browser Cookies Discussion**
- **Glossary**



# PERSONAL GUIDING PHILOSOPHY

***"My intellectual property is the source of my income therefore I will properly maintain and protect it!"***





# Preventative Maintenance Steps

## ■ To aid in preventing and recovering from system problems:

- Perform routine system and data file backups!
  - ❖ More on this topic later
- Perform routine disk file and file directory defragmenting!
  - ❖ Preferably using a qualified 3<sup>rd</sup> party program (not Windows std. Defrag utility)
  - ❖ Online & Offline defrag (offline avail. only if using Exec. S/W Diskeeper)
  - ❖ Check file system integrity before and after defrag
  - ❖ More on this topic later



## Preventative Maintenance Steps (Cont'd)

### ■ To aid in preventing and recovering from system problems (Cont'd):

- For NT/Win2K/WinXP systems:  
periodically review System and Application Event logs (Event Viewer)
  - ❖ First place to look if system or application problems occur
  - ❖ Insure that both Logs are configured to save collected event data to a 4 MB min. file size (requires configuration, not the default)
  - ❖ Check for any abnormal (red or yellow icon) events, and try to determine source of problem





## Preventative Maintenance Steps (Cont'd)

### ■ To aid in preventing and recovering from system problems (Cont'd):

- At least once every 2-6 months
  - ❖ Run a manual AUTOCHK/CHKDSK file system integrity check on each disk partition in the sys.
    - Use either File Explorer > Properties > Tools > Error-checking > Check now & select fix file errors + scan for and attempt recovery of bad sectors
    - Or use an optional 3<sup>rd</sup> party app such as Exec. S/W Diskeeper to perform a CHKDSK followed by offline boot-time defrag of each partition



## Preventative Maintenance Steps (Cont'd)

### ■ To aid in preventing and recovering from system problems (Cont'd):

- At least once every 2 months
  - ❖ Perform an online and offline (avail. with Diskkeeper only) defrag for each disk partition in the system
  - ❖ If defrag was extensive then after defrag run AUTOCHK/CHKDSK again on each partition to check file integrity
- After any AUTOCHK/CHKDSK file system integrity check
  - ❖ Review AUTOCHK entries in the Application Event log to see if there are any problems or anomalies (such as bad blocks)



# Backup and Disaster Recovery Considerations

## ■ Backup Considerations

- Use a commercially available 3<sup>rd</sup> party online backup program
  - ❖ Regularly perform backup on time or event-based schedule
  - ❖ Back up system and data files to prepare for Disaster Recovery
  - ❖ Backup types: normal or full (recycle\*), incremental, and differential (normal\*)
  - ❖ Perform backup and a test file restore using the selected backup media
- Select backup device and media for maximum portability between diff. PC's
  - ❖ Suggested media: CD-R or CD-RW, cartridge tape, and internal hard drive reserved for backup use only

\*Dantz Retrospect terminology





# Backup and Disaster Recovery Considerations (Cont'd)

## ■ Disaster Recovery Considerations

- What is Disaster Recovery?
  - ❖ Capability to restore all system and data files in event of partial or full PC system failure
  - ❖ Typical “disasters” that may occur: complete hard drive failure (boot and data drives-after replacement), hard drive boot sector corruption, OS corruption preventing restart, etc.
- Use a commercially available 3<sup>rd</sup> party online backup program with base or opt. Disaster Recovery cap.
  - ❖ Make an explicit Dis. Rec. Backup (requires Windows installation CD & valid OS lic. #)
  - ❖ Store Dis. Rec. emergency boot CD along with data + system backup media in a secure location



# Security & Integrity Considerations

## ■ System Security Considerations

- System security--protect your system against:
  - ❖ Malicious acts, identity theft (use ID & secure password for all Internet accts plus use secure PC startup/logon)
  - ❖ Internet hackers (personal firewall highly reco'd)
  - ❖ Virus intrusions (anti-virus pgm that scans email with data tables updated biweekly - abs. must!)
  - ❖ Sabotage/theft/intentional destruction of intellectual property (store Dis. Rec. backup offsite, consider a home security system with intrusion alarm auto-dial to a security agency)
  - ❖ Privacy intrusions and unapproved access of personal info. (configure your internet browser for enhanced security and privacy; consider investing in privacy protection utility apps)



# Security & Integrity Considerations (Cont'd)

## ■ System Integrity Considerations

- System integrity--protect your system against:
  - ❖ Power surges, blackouts, brownouts (surge protector min., UPS highly reco'd)
  - ❖ Fire & smoke damage (install a sep. smoke detector in PC room, purchase an electronics-compatible fire extinguisher and keep near PC system, consider a home security system with fire alarm and auto-dial to a security agency)
  - ❖ Inadvertent file deletion, system software corruption, system destruction & force majeure (use Norton Utilities WinDoctor, make routine system backups, and periodically store and update backup set in a secure offsite location such as a bank safe dep. box)





## Useful Third Party Software Utility Apps

### ■ Symantec Norton Anti-Virus (NAV)

- Versions: 2003 Std. (\$50), Pro (\$70)

### ■ Symantec Norton Utilities (NU)

- Versions: 2003 Std. (\$70), Pro (\$100)
- More comprehensive alt.: Norton Systems Works, Vers. Pro 2003 (\$100.)
- NAV & NU are included in Norton SystemWorks

### ■ Executive Software Diskeeper

- Workstation 7.0 (\$48), XP Server 7.0 (\$233), Small Biz 7.0 (\$301) versions

### ■ Dantz Retrospect Backup

- Requires a compatible backup device such as a Dantz Retrospect-approved CD-RW or cartridge tape drive
- Versions: Pro (\$88), Single Server (\$463), Multi Server (\$727) + Dis. Rec. Opt. for Servers only (already included in Pro vers.) (\$414)
- Alt.: Veritas Backup Exec (more expensive)

Gen'l software pricing ref.: <http://www.computers4sure.com/>



## Useful Third Party Software Utility Apps (Cont'd)

### ■ Norton Personal Firewall

- Version: 2003 Std. (\$50)

### ■ Ontrack Data Int'l Internet Cleanup

- Version: 2.0 (\$30) works with Win 95/98/Me/NT4.0/2000/XP (use with XP may not be supported by the developer)
- Very useful for Web Browser Cookie, Cache & History Management & Cleanup
- Can be purchased from Amazon.com (search for On-Track Internet Cleanup 2.0 in the Software category)
- Reported in Amazon.com that it does not work with AOL 7.0 (also there may be problems with other AOL versions?)
- Alt.: Internet Eraser Pro (\$80) (no author's personal experience using it)

### ■ Roxio Easy CD Creator

- Reco'd version: Platinum 5.0 (\$80)
- Requires a compatible CD-RW drive

### ■ WinZip Computing WinZip

- Version: Std. (\$15)



## Useful Third Party Software Utility Apps (Cont'd)

### ■ Failsafe Technologies Guard-IE

- Current Version: 3.2 (\$30)
- For Internet Explorer V5.0 SP2 and higher, can optionally:
  - ❖ Prevent browser pop-ups and pop-downs
  - ❖ Prevent script-driven ads & the “hijacking” of your browser
  - ❖ Intercept potentially hostile script-based attacks (such as Active-X or JavaScript) that can infect your computer simply by Web browsing
  - ❖ Remove all traces of your Web activity
  - ❖ Erase some or all of web browsing tracks such as: cookies and temp files, previous form entries, typed URLs, passwords, etc.
  - ❖ Remove and/or prevent the new class of browser privacy invasion tools from being used to secretly store data on your computer
- Fully integrates into IE V5.0 SP2 and higher with a ‘control panel’ icon that is automatically inserted in the browser toolbar
- Can be securely purchased and downloaded online from:  
<http://www.guardwall.com/en/index.asp>



# Internet Browser Cookies Discussion

## ■ Introduction to Cookies

- The WWW is built on a very simple, but powerful premise. All material on the Web is formatted in a uniform format called HTML (Hypertext Markup Language), and all information requests and responses conform to a similarly standard protocol. Cookies are pieces of information generated by a Web server and stored by the Web server using the user's Web browser (e.g., Internet Explorer or Netscape) in the user's computer, ready for future access. Cookies are embedded in the HTML information flowing back and forth between the user's computer and the servers. Cookies were implemented to allow user-side customization of Web information. For example, cookies are used to personalize Web search engines, and to store shopping cart items a user has selected while browsing through a virtual shopping mall. Cookies are stored by the user's Web browser on the user's system disk in the user's designated Cookies folder, and are loaded into the Web browser's memory when the browser is started. Cookies utilize user-specific info. transmitted by the Web server onto the user's computer so that this info. will be available for later access by itself or other servers.



# Internet Browser Cookies Discussion (Cont'd)

## ■ Introduction to Cookies (Cont'd)

- In most cases, not only does the storage of personal information into a cookie go unnoticed, so does access to it. Web servers automatically gain access to relevant cookies whenever the user establishes a connection to the Web Server, usually in the form of Web requests. For more info. on Cookies, access this web site URL: <http://www.cookiecentral.com/>, and click on the FAQ tab. Copyright/Credits for above info. (edited and expanded by the author): Viktor Mayer-Schönberger and David Whalen.

**Author's Usage Notes:** 1. For Internet Explorer (IE), do not delete cookies using the std. file delete command to delete 'user@cookie\_filename.txt' files in the Cookies folder. This is because IE maintains a user Cookies folder index file (index.dat) and loads cookies according to the info. stored into that file (which is a binary file that is continuously in use and so cannot be accessed or altered by the user.) If it is desired to delete ALL cookies (refer to below caveat 1st), first back them up to a text file using the IE Command File > Import and Export...> Export Cookies.





# Internet Browser Cookies Discussion (Cont'd)

## ■ Cookies (Cont'd)

**Author's Usage Notes (1. Cont'd):** Choose the file location, and after using the Wizard and clicking on Finish, IE will export them to a readable text file that is default named as 'cookies.txt.' Then use Tools > Internet Options, click on the General tab, and under the 'Temporary Internet Files' area, click on the Delete Cookies... button. **Caveat: this command will delete ALL cookies, which is most generally not desirable** since some cookies are used to store info. such as web site access codes and user ID info. that may be necessary to use that site. A much better method is to use a 3<sup>rd</sup> party utility program such as Ontrack Internet Cleanup so that individual cookies can be backed up (using the Save cmd.) if desired, then deleted (and optionally shredded as well.) Also note that if cookies are accidentally deleted using IE or a 3<sup>rd</sup> party utility program, and they were not previously saved using IE or a 3<sup>rd</sup> party utility program, then simply restoring the deleted cookie file(s) to the user's Cookies folder will NOT result in IE recognizing the restored cookie (due to an index.dat file conflict.)



# Internet Browser Cookies Discussion (Cont'd)

## ■ Cookies (Cont'd)

Author's Usage Notes (Cont'd): 2. It is recommended to enhance protection of your privacy and security that you take the following steps:

- **Block 3<sup>rd</sup> Party Cookies.** For Internet Explorer, this can be done by using Tools > Internet Options and clicking on the 'Privacy' tab, then clicking on the 'Advanced' button, and configuring how cookies are to be handled. An example of this configuration is shown as an Addendum on the following slide.
- **Consider purchasing, installing and properly configuring Norton Personal Firewall (included in the list of Useful Third Party Software Utility Apps in a previous slide.)** This utility program, if properly installed, configured, and routinely updated can be used to greatly enhance the user's PC security and privacy; as well as to make the PC more resistant to certain classes of attacks by hackers. This app will "plug-and-play" properly with Internet Explorer, Ontrack Internet Cleanup, Norton Anti-Virus, and the supported versions of Microsoft Windows operating systems.

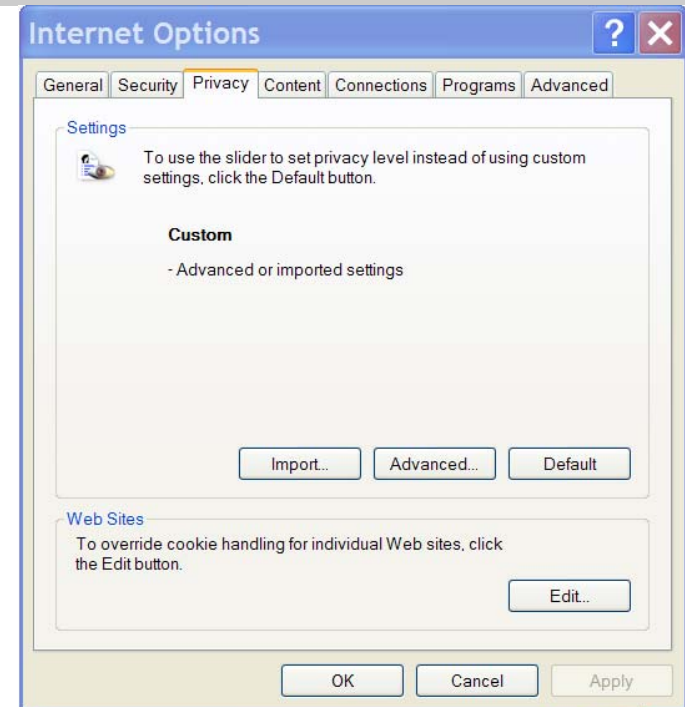


# Internet Browser Cookies Discussion (Cont'd)

## ■ Cookies (Cont'd)

### Author's Usage Notes (2. Cont'd): Addendum.

- An example of Internet Explorer V6.0 Advanced Privacy Settings that are configured to override automatic cookie handling and prescribe how cookies are handled is shown here:





# Internet Browser Cookies Discussion (Cont'd)

## ■ Cookies (Cont'd)

Author's Usage Notes (Cont'd): 3. Note that there are actually two types of JavaScript cookies that can be implemented by web servers: permanent, and session-only.

- Permanent cookies store information in a physical file that is automatically installed (unless the user or a previously installed 3<sup>rd</sup> party privacy protection program intervenes) in the user's computer. For IE V5.0 and above, this file is named 'user@cookie\_filename.txt' and is always installed in the logged on user's Cookies folder. This stored data then becomes "permanently" available to [supposedly] only the web server that stored the cookie
- Session-only cookies store information only in the browser memory, and this info. is only available for the duration of the browser session. In other words, the data that is stored inside a session-only cookie is available from the time of storage until the browser window is closed. Moving from web page to page during the time that the browser is open does not erase the data temporarily stored by a session-only cookie.



# Glossary

Definitions ref.: <http://whatis.techtarget.com/>

- **SOHO** – Small Office or Home Office
- **Graphical User Interface (GUI)** – the means of communicating to a computer using images and text, instead of only using (sometimes cryptic) text programming commands, e.g. in the early days of Microsoft DOS-based PC's that had no GUI.
- **Multitasking** – the operating system's capability to have pre-emptive, time-sliced, priority-driven program execution.
- **Multithreading** – the operating system's capability to have multiple subpgms executing independently. Note that a single thread cannot span multi-processors, however different threads can be run in different processors to improve performance.



# Glossary (Cont'd)

- **Network** – A group of computers that are connected in order to communicate.
- **Protocol** – a set of rules and standards for network communication.
- **TCP/IP** – Transmission Control Protocol/Internet Protocol, the standard protocol used for Internet communications worldwide.
- **DNS** – Domain Name System – associates network TCP/IP addresses with computer names. If there is no DNS, then the network Hosts table in each PC performs this function.
- **FTP** – File Transfer Protocol – a commonly used protocol used to transfer files from one computer to another, esp. on the Internet.



## Glossary (Cont'd)

- **Domain** – a collection of users and computer hardware that are controlled and administered with a Primary Domain Controller or PDC (and optionally a Backup Domain Controller or BDC), in order to communicate and share common resources.
- **ISA** – Industry Standard Architecture. ISA is a standard bus (computer interconnection) architecture that was originally associated with the IBM AT motherboard. ISA is an older and slower PC device interface standard than the currently used PCI interface std, so is rarely used in current PC architectures. It is common to refer to PC device interface card slots with an ISA architecture as ISA slots.
- **PCI** – Peripheral Component Interface. The internal PC card expansion bus now in most popular use. PCI is a way of interconnecting a microprocessor and attached devices, in which expansion slots are spaced closely for high speed operation. It is common to refer to PC device interface card slots with an PCI architecture as PCI slots.



## Glossary (Cont'd)

- **IDE** – Integrated Drive Electronics. IDE is a standard electronic interface used between a computer motherboard's data paths or bus and the computer's disk storage devices. Most computers sold today use an enhanced version of IDE called Enhanced Integrated Drive Electronics (EIDE.)
- **ATAPI** – AT Attachment Packet Interface. ATAPI is an interface between a computer and attached peripheral devices. Most of today's computers use the standard Integrated Drive Electronics (IDE) interface to address hard disk drives. ATAPI provides the additional commands (above IDE and EIDE) needed for controlling a CD-ROM player or tape backup so that a computer can use the IDE interface and controllers to control these device types.





## Glossary (Cont'd)

- **SCSI** – Small Computer Systems Interface, an older but ever evolving set of standards and protocols to be interfaced to a PC with high standards that allow peripheral devices such as hard drives speed data transfer. Requires that a SCSI adapter card be installed in the PC, and special SCSI cables that match the peripheral device(s) connector type(s.)
- **USB** – Universal Serial Bus. a plug-and-play interface between a computer and add-on devices. With USB, a new device can be added to a PC without having to add an adapter card or even having to turn the computer off. A different plug-and-play standard, IEEE 1394, supports much higher data rates and devices such as video camcorders and digital video disk (DVD) players. However, USB and IEEE 1394 serve different device types.

