

CONTACT Information

Toll Free - 888.857.8808
Local - 616.997.TECH(8324)
Fax - 616.997.9317
Email Sales - sales@ccstech.net
Email Information - info@ccstech.net
Technical Support - support@ccstech.net

President

Greg Slater - gslater@ccstech.net

IT Client Managers

Ryan McMillen - rcmillen@ccstech.net
Gary Slager - gslager@ccstech.net
Karen Strickland - kstrickland@ccstech.net
Scott Toney - stoney@ccstech.net
Joe Vanderstelt - jvanderstelt@ccstech.net
Jeff Verry - jverry@ccstech.net

Back issues: www.ccstech.net/news.htm

Complete Workstation Backup System \$249.99

Acronis Workstation Software

- Enterprise level protection
- Laptop or Desktop Computer
- Electronic image of entire hard drive
- Backs up every file and system files
- No need to reinstall programs
- Recovers your entire system in minutes

One Year Acronis upgrades & support
Lacie 250GB External Hard Drive
*We use it ourselves!
Ask about installation.*

\$100 for Trade-In PC

For a limited time we will give you \$100 off the price of this \$699 Acer computer when you trade-in your old PC (in any condition, no exceptions)

Only one-third the size of a traditional desktop computer, this compact business computer may be small in size but it is big on computing power and features.

Windows XP Professional Downgrade Preinstalled, Intel® Core™2 Duo (3MB L2 cache, 2.80GHz, 1066MHz FSB), 2GB (2/0) DDR2 SDRAM, 160GB SATA hard drive, Super-Multi drive with LabelFlash™, multi-in-one card reader, NVIDIA® GeForce® 7100 graphics, gigabit LAN



Setup and Ready to Use!
Offer good 8/12/09 thru 8/31/09 or while supplies last.

Risk Assessment Review

by Karen Strickland

► There are many threats to computer users and data existing today. These threats come from both external and internal sources. Some are intentional, some are not.

External Threats

External threats are those that originate outside of your computer environment. Some obvious threats that you may not think about are thieves and natural disasters. Both may result in loss of equipment and/or data. However, the most well known examples of external threats are viruses and spyware. You may not realize it, but in the fight between security software and malicious software (viruses, spyware, etc.), the bad guys are winning! Unfortunately, they seem to have a fairly accurate handle on how the average person thinks. They are constantly coming up with new schemes to convince computer users to click on the wrong link, go to the wrong website, or run a program that looks totally legitimate but isn't. It is very possible that you may not even have to click on anything to get infected, all you have to do is go to the wrong website.



Hackers are another external threat. Many seem to feel it a challenge to try a direct attack on a computer. They use various scripts and programs that they have written to try to guess your password. Once they have that, getting your information may not be difficult at all.

Internal Threats

Outside attacks are not the only threats that you need to be concerned with. There are also threats that come from inside your organization whether that is an office or your home. Unfortunately, there is a lot of down-sizing and turn-around in jobs today. Unless there is tight control of computer access during a separation of employment, there is a chance that someone could use his or her anger to damage your computer or information.



Damage to a computer system can be totally unintentional as well. When updates to software on your computer are performed there is always a slight risk that something will go wrong. Usually that is easily corrected by uninstalling the update, but that is not a guarantee.

Access to a business computer by non-employees can be a threat as well. In a home office that could be your children, their friends, or any visiting relative. Anything that they may innocently load, be it a game, screen saver, movie or song could be a threat.

There are a couple steps that you can take to help protect your computer against these threats no matter what your situation.

Step #1: The only sure way of protecting your data is to make sure you have restorable backups. We recommend a product called *Acronis* for creating image based backups of your system. When your system is damaged by any internal or external threat, it may not be repairable and in that case, your only means of recovery is going to be to restore from an earlier backup to remove the damage or the infection. For more information regarding backups, go to our website (www.ccstech.net) and read the March 2009 newsletter under the "News" page. It does an excellent job of explaining how the proper backups are the "Cheapest Insurance You Can Buy".

Step #2: Particularly important for those with a home-office, is to keep your business computer exactly that. Don't allow non-business activities to be performed on it. If at all possible, have another computer that the kids (and friends) can use for their internet activities. If this isn't possible, refer back to Step #1.

If you are not sure you're protected from internal or external threats give us a call right away. We can help make sure that you are protected!

"Relax...we're on IT"

Joe's Tip: Default Deny by Joe Vanderstelt

► **Default Deny- "Everything, not explicitly permitted, is forbidden".**

Many of our clients view their anti-virus software and firewall like bouncers for a club. They remove threats and keep them out. Well behaved individuals can freely come and go without much trouble. **Default Allow** security policies are a lot like this. Like the patrons of a club, well behaved employees can freely visit websites and run software unless it interferes with a system required for their business. This approach works well, the employees feel safe, and the security does not interfere with functionality.

But you would not want to take the "bouncers" approach with your home. There you only want people to gain

entrance if you give them expressed permission. The **Default Deny** approach is like an alarm system. Only people with the key code can enter. Applied to your network, only employees with permission can visit a website, only employees with permission can install and run software.

Default Deny is significantly more secure than **Default Allow**, but for that security you sacrifice ease of use and functionality. **Default Deny** is used by some of our larger customers and to keep them safe. *CCS Technologies* can help you determine which is most appropriate for your environment and assist you with implementing it.

"Relax...we're on IT"