DCSI Security Baseline

1. Hardware Firewall. You should have a hardware firewall, such as a Linksys router. Windows' software firewall should be turned off. The hardware firewall may have to be configured to allow remote access via PC-Anywhere or VNC. If you are using a wireless access point (WAP), make sure that the SSID broadcast is turned off and be sure to enable WPA or WPA2, which provide strong Wi-Fi security.

2. Anti Virus Software. I prefer Trend Micro's PC-cillin Internet Security suite. It includes Anti-Spyware and Anti-Spam. The software subscription should be renewed annually and updated automatically. A full system scan should be run on every computer in the office once a week. The software should be configured to effectively balance protection and performance.

TREND MICRO™

3. Update Management. Windows Update and Microsoft Update are not recommended. To protect against questionable Microsoft downloads, knowledgeable users should configure automatic updates to "Notify me but don't automatically download or install". Only install patches which have been reviewed before installing. I subscribe to a patch management newsletter. I then use Shavlik's NetChk Protect to identify missing service packs and patches and to deploy critical patches once a month.

4. Business Computer Usage Policy. You should have a written computer usage policy that is reviewed with your staff at least once a year. It should have clear guidelines for what personal use of business computers is permitted and what is forbidden. Work computers should be used for business use only. Shopping and surfing the internet put computers at risk for malware and other attacks. Opening unknown messages and accessing web sites from links inside e-mails open your computers to viruses, cyber-crimes and other threats. Non employees (including patients and family members) should never use business computers (including laptops).

dcsi

Charlie Kleiman
Dental Computer Systems Integration
www.dcsiDental.com
415-491-1930
October 2006