Protocols for a "Computer Code Blue"

Sunday, April 10, 2005
12:23 PM

1. First, don't make the situation any worse! I have seen a number of cases where well-meaning people have turned a simple problem into a real catastrophe. Doing nothing at all is frustrating but it is sometimes the best and safest course.
2. Read all of these suggestions before you do anything else!
3. Look for simply things first. Is it plugged in, is it turned on, etc. Power cables work lose! Be sure all cables and connectors are completely seated.
4. If you have a support agreement with an IT person, call her/him now! Often, things can be fixed over the telephone or Internet. Your IT person should have provided you with diagram of your office computer system showing how the computers, printers, backup, firewall and Internet connection are actually configured. This information is invaluable, especially at a time like this. Be sure to mention to your emergency IT person that you have such documents. If you do not have such documents, this is the first thing you want your new IT person to provide for you after the emergency is over!
5. Think about any changes that have been made to your system? Did anyone install new software, an update, or add a new printer, etc? Anyone been "surfing" on the Internet? (Especially common with "Associate" dentists!) Do not try to fix these problems yourself but be sure to mention any changes to your IT person.
6. If you must attempt a "restore," do not, under any circumstances, attempt the restore on your file server! If necessary, go buy a brand new computer and attempt the restore on that one first. I have seen several cases where a defective backup over-wrote data that could easily have been saved. At the very least, you will lose some data when you restore a backup. (If your IT person suggests restoring your backup on your server, immediately hire a new IT person! Absolutely no exceptions!)
7. Do some computers on the network still work, while others do not? Then you do not have a "server" problem! Disconnect the non-working computers from your network (or simply unplug them from the wall). Work with the computers that still function until qualified help arrives.
8. If no computers work, check your "hub" or "switch" first. This is the central connection for all your computer cables. Is it plugged in? Are its lights flashing? You will generally not harm anything by simply unplugging the electrical supply to the hub, waiting 30 seconds, and then plugging it back in again. (This is known as "rebooting the hub" … and sometimes works but has no risks associated with it)
9. Check, but do not change, the file server: plugged in, lights on, etc. What shows up on the monitor? DO NOT CHANGE ANYTHING ON THE SERVER WITHOUT SPECIFIC INSTRUCTIONS FROM YOUR NETWORK ADMINISTRATOR! (Your "network administrator" is your IT person, not the "office manager" or "dentist.")
10. If both your file server and hub/switch appear to be working, do a "cold boot" on one workstation. To be sure you are doing a true cold boot, unplug the computer from the electrical outlet, wait 30 seconds, then plug it back in and turn it on. If you do not actually unplug the computer from the wall and wait 30 seconds, you have not done this step correctly!
11. If you have an in-office computer-to-computer backup system, you may wish

11. to switch to this system for “read only” use. This means you can look up information but not change any information. Any changes made to this data will be lost! And any changes made on your regular system since this backup was made will not show up here so use this cautiously!
12. Keep in mind that a “crashed” system can almost always be “resuscitated” by data salvage companies such as DriveSavers (www.drivesavers.com; 800.440.1904). It may take a few days and cost a few thousand dollars but it is better than losing all your data! If things “aren’t going well,” you should at least give them a call and get some additional advice!
13. Work with a qualified IT person! There are lots of very knowledgeable IT people who are very competent but do not have an MCSE certification. And the fact that someone does have an MCSE certification does not mean they won’t cheat you. But it does mean they have done some studying and passed a fairly rigorous series of tests. All other things being equal, an MCSE person is probably your best bet in a “computer code blue” situation.
14. When the emergency is over, sit down with your IT person and try to prevent the next emergency!
    a. Setup an off-site “clone” system and use “stem cell” backups which you test at least weekly (http://www.painlesscom.com/backup%20clones%20and%20stem%20cells.pdf)
    b. A diagram of your computer system showing all computers, printers, backup, firewall, internet connections, modems, IP addresses, computer names, administrator passwords (store this document in a safe, secure location)
    c. An on-site computer-to-computer nightly backup system
    d. Some off-site monitoring of your system over the Internet by your IT service
    e. A maintenance / support agreement which includes installation of all updates and new software
    f. Hardware firewall and virus / spyware protection
    g. Access control of your Internet connection (a “white list” administered by the owner-dentist should be considered)
    h. “Strong” passwords and encryption of all patient data
    i. Encryption of all email containing patient information
    j. A discussion of the new (April 05) HIPAA Security requirements
    k. Physical protection of all computers containing patient data (bicycle lock-type devices)