minated, whether they are coax, Cat5e, or fiber optics. Inexpensive testers are available for electrical cables and fiber links can be tested with a flashlight. Bad cabling and connectors account for up to 50 percent of networking problems. Get the simple stuff out of the way and test each cable before connection into IP electronic devices.

6. **Leaving IP devices on the factory defaulted Port 80.** There are 65,535 software ports available in TCP/IP LAN and Internet connectivity. Most of our vendors ship their IP video devices such as NVRs, DVRS, and cameras default programmed to port #80, which is commonly referred to as the "http" or Hypertext Transfer Protocol port. While using this port makes it a bit easier for clients to access devices on the LAN, if the device is to be available over the Internet, using port 80 makes it very easy for hackers to find the device on the local network and attempt to take it over. Common hacking software such as NMAP will scan the first 1500 ports if a hacker tries a "quick scan." If technicians select port numbers higher than 1600, typically a hacker will need to scan all 65,535 ports, which can take hours. Selecting high port numbers provides the IP device with "security through obscurity." And, remember, if there are multiple IP devices that need to be accessed from the Internet, each device must be on a unique port number(s).

7. **Not taking a snapshot of the system once it's functional.** After an installation has been performed and everything is working correctly, most security installation companies would pack up their gear and head for the next job. Remember that if you are using the client's network and/or Internet connection, any changes to the network configuration may well spell trouble for the IP physical security devices. Smart installation companies take a "snapshot" of the network once everything is working, using either freeware software such as NMAP/ZENMAP or higher-end programs such as IntraVue. However you do it, it's very important to take a picture of the network when it is working properly. Then if there are problems, take another snapshot and compare the two. In many cases you'll find that the network and/or firewall has been reconfigured and needs to be changed to allow the proper communication of the IP security devices.

While none of us is perfect, we can perform perfect installations of IP security devices if we follow the rules and avoid the mistakes detailed above. Do it right the first time and your profitably is assured.