

By Debra Littlejohn Shinder, MVP, MCSE

Every general computer networking class teaches the OSI and/or DoD networking models, and we all learn that everything begins at the bottom, with the physical level. Likewise, when it comes to IT security, physical security is the foundation for our overall strategy. But some organizations, distracted by the more sophisticated features of software-based security products, may overlook the importance of ensuring that the network and its components have been protected at the physical level.

In this article, we'll take a look at 10 of the most essential security measures you should implement now, if you haven't already done so.

1 Lock up the server room

Even before you lock down the servers, in fact, before you even turn them on for the first time, you should ensure that there are good locks on the server room door. Of course, the best lock in the world does no good if it isn't used, so you also need policies requiring that those doors be locked any time the room is unoccupied, and the policies should set out who has the key or keycode to get in.

The server room is the heart of your physical network, and someone with physical access to the servers, switches, routers, cables and other devices in that room can do enormous damage.

2 Set up surveillance

Locking the door to the server room is a good first step, but someone could break in, or someone who has authorized access could misuse that authority. You need a way to know who goes in and out and when. A log book for signing in and out is the most elemental way to accomplish this, but it has a lot of drawbacks. A person with malicious intent is likely to just bypass it.

A better solution than the log book is an authentication system incorporated into the locking devices, so that a smart card, token, or biometric scan is required to unlock the doors, and a record is made of the identity of each person who enters.

A video surveillance camera, placed in a location that makes it difficult to tamper with or disable (or even to find) but gives a good view of persons entering and leaving should supplement the log book or electronic access system. Surveillance cams can monitor continuously, or they can use motion detection technology to record only when someone is moving about. They can even be set up to send e-mail or cell phone notification if motion is detected when it shouldn't be (such as after hours).

3 Make sure the most vulnerable devices are in that locked room

Remember, it's not just the servers you have to worry about. A hacker can plug a laptop into a hub and use sniffer software to capture data traveling across the network. Make sure that as many of your network devices as possible are in that locked room, or if they need to be in a different area, in a locked closet elsewhere in the building.

4 Use rack mount servers

Rack mount servers not only take up less server room real estate; they are also easier to secure. Although smaller and arguably lighter than (some) tower systems, they can easily be locked into closed racks that, once loaded with several servers, can then be bolted to the floor, making the entire package almost impossible to move, much less to steal.

5 Don't forget the workstations

Hackers can use any unsecured computer that's connected to the network to access or delete information that's important to your business. Workstations at unoccupied desks or in empty offices (such as those used by employees who are on vacation or have left the company and not yet been replaced) or at locations easily accessible to outsiders, such as the front receptionist's desk, are particularly vulnerable.

Disconnect and/or remove computers that aren't being used and/or lock the doors of empty offices, including those that are temporarily empty while an employee is at lunch or out sick. Equip computers that must remain in open areas, sometimes out of view of employees, with smart card or biometric readers so that it's more difficult for unauthorized persons to log on.

6 Keep intruders from opening the case

Both servers and workstations should be protected from thieves who can open the case and grab the hard drive. It's much easier to make off with a hard disk in your pocket than to carry a full tower off the premises. Many computers come with case locks to prevent opening the case without a key.

You can get locking kits from a variety of sources for very low cost, such as the one at [Innovative Security Products](#).

7 Protect the portables

Laptops and handheld computers pose special physical security risks. A thief can easily steal the entire computer, including any data stored on its disk as well as network logon passwords that may be saved. If employees use laptops at their desks, they should take them with them when they leave or secure them to a permanent fixture with a cable lock, such as the one at [PC Guardian](#).

Handhelds can be locked in a drawer or safe or just slipped into a pocket and carried on your person when you leave the area. Motion sensing alarms such as the one at [SecurityKit.com](#) are also available to alert you if your portable is moved.

For portables that contain sensitive information, full disk encryption, biometric readers, and software that "phones home" if the stolen laptop connects to the Internet can supplement physical precautions.

8 Pack up the backups

Backing up important data is an essential element in disaster recovery, but don't forget that the information on those backup tapes, disks, or discs can be stolen and used by someone outside the company. Many IT administrators keep the backups next to the server in the server room. They should be locked in a drawer or safe at the very least. Ideally, a set of backups should be kept off site, and you must take care to ensure that they are secured in that offsite location.

Don't overlook the fact that some workers may back up their work on floppy disks, USB keys, or external hard disks. If this practice is allowed or encouraged, be sure to have policies requiring that the backups be locked up at all times.

9 Disable the drives

If you don't want employees copying company information to removable media, you can disable or remove floppy drives, USB ports, and other means of connecting external drives. Simply disconnecting the cables may not deter technically savvy workers. Some organizations go so far as to fill ports with glue or other substances to permanently prevent their use, although there are software mechanisms that disallow it. [Disk locks](#), such as the one at [SecurityKit.com](#), can be inserted into floppy drives on those computers that still have them to lock out other diskettes.

10 Protect your printers

You might not think about printers posing a security risk, but many of today's printers store document contents in their own on-board memories. If a hacker steals the printer and accesses that memory, he or she may be able to make copies of recently printed documents. Printers, like servers and workstations that store important information, should be located in secure locations and bolted down so nobody can walk off with them.

Also think about the physical security of documents that workers print out, especially extra copies or copies that don't print perfectly and may be just abandoned at the printer or thrown intact into the trash can where they can be retrieved. It's best to implement a policy of immediately shredding any unwanted printed documents, even those that don't contain confidential information. This establishes a habit and frees the end user of the responsibility for determining whether a document should be shredded.

Summary

Remember that network security starts at the physical level. All the firewalls in the world won't stop an intruder who is able to gain physical access to your network and computers, so lock up as well as lock down.



Debra Littlejohn Shinder is a technology consultant, trainer and writer who has authored a number of books on computer operating systems, networking, and security. These include *Scene of the Cybercrime: Computer Forensics Handbook*, published by Syngress, and *Computer Networking Essentials*, published by Cisco Press. She is co-author, with her husband, Dr. Thomas Shinder, of *Troubleshooting Windows 2000 TCP/IP*, the best-selling *Configuring ISA Server 2000*, and *ISA Server and Beyond*.

Additional resources

- TechRepublic's [Downloads RSS Feed](#) **XML**
- Sign up for TechRepublic's [Downloads Weekly Update](#) newsletter
- Sign up for our [IT Management NetNote](#)
- Check out all of TechRepublic's [free newsletters](#)
- [Take security precautions when an employee leaves the organization](#) (TechRepublic download)
- [10 things you can do to protect your data](#) (TechRepublic download)
- [Protect your organization against pretexters with help from Sun Tzu and The Art of War](#) (TechRepublic download)

Version history

Version: 1.0

Published: July 16, 2007

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team