BLACK BOX
NETWORK SERVICES

Physical Network Security

Network security from the bottom up

Before the firewall, consider the lock.

Table of Contents

Introduction 3
The goal of network security 3
Layered security—using the OSI model as a security model 4
Why physical access to computers is a problem 5
Lock it up! 5
Security cameras 8
Secure your in/out devices 9
Use fibre optic cable 10
Protect data 10
Protect equipment from accidental damage 11
Treat wireless with care 13
Don't forget the paper trail 13
The most vulnerable security gap—humans 13
In conclusion 13
About Black Box 13

We're here to help! If you have any questions about your application, our products, or this white paper, contact Black Box Tech Support on 0118 965 6000 or go to www.blackbox.co.uk and click on "Need Help?." You'll be live with one of our technical experts in less than 20 seconds.

Introduction

Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.

From "10 Immutable Laws of Security," Microsoft® Security Response Centre

It has been said that the most secure computer is one that's by itself in a locked room. It should be turned off.

Obviously, this is not a computing situation that's going to work for most organisations, but the general idea that isolating computers increases security holds true. The most basic step you can take towards network security is to secure your hardware so unauthorised people can't get at it.

Securing hardware is important because if a person has physical access to a device, there is almost always a way to take control of it or to get data out of it.

It's at the hardware level, the very bottom of the networking hierarchy, that your network is most vulnerable. A lost laptop, an open USB port, a simple network tap—all these can be a conduit for quick and devastating data loss that no firewall can prevent.

But the hardware arena is also where you can set up the most effective network security by denying physical access to networking devices. There are many ways to ensure the physical security of your network, from simple port locks to sophisticated remote monitoring systems. What they all have in common is that they limit access to network hardware to prevent unauthorised alteration to network devices or the theft of data.

This white paper explores ways to improve network security through basic physical security. Whether you're protecting government secrets, complying with HIPAA requirements, or keeping financial information private, you need to first look at who can physically access your network.

The goal of network security

Network security should ensure that authorised users get convenient and easy access to information, while preventing unauthorised access or tampering. This is often expressed as confidentiality, integrity, and availability (CIA). Confidentiality is preventing unauthorised personnel from getting private information; integrity is preventing unauthorised personnel from altering information; and availability is ensuring that information is available to authorised personnel when it's needed.

Network security means allowing the right people to access the right information at the right time. It can be a fine balancing act to protect data and keep out the unwanted while still enabling your staff to get work done without undue encumberment.

It's important to ensure that computers and network equipment are physically protected to a degree that's consistent with their value.

In short, the goal of network security is to provide maximum confidentiality, integrity, and availability while balancing cost and risk.

Layered security—using the OSI model as a security model

Network security is often based on the familiar OSI model, which organises networking into seven layers. When information travels from one network node to another, its control is passed from one layer to the next, starting at Layer 7 at the transmitting node, traveling down to Layer 1, crossing to the next node, and then going from Layer 1 back up to Layer 7 at the receiving node.

The OSI Layers are:

Layer 1, the Physical Layer: Defines such electrical and mechanical characteristics of networking equipment as voltage levels, signal timing, data rate, maximum transmission length, transmission media, network topology, and physical connectors.

Layer 2, the Data Link Layer: Here data packets are encoded and decoded.

Layer 3, the Network Layer: Includes switching and routing protocols.

Layer 4, the Transport Layer: Provides for the transparent transfer of data between nodes, as well as error recovery and flow control.

Layer 5, the Session Layer: Establishes, manages, and terminates connections.

Layer 6, the Presentation Layer: Formats data to be sent across a network to ensure there are no compatibility problems.

Layer 7, the Application Layer: Supports applications and end-user processes.

A complete network security plan addresses security at all OSI layers, starting at Layer 1 with securing the hardware and working up through the layers to include password protection, encryption, VPNs, virus scans, and firewalls.

A security barrier at each Layer protects against all kinds of attacks and provides complete network security.

Layer 1 security can loosely be defined as physical security—keeping persons physically away from the hardware that holds unauthorized data and also protecting that hardware from deliberate or accidental damage.

Network security starts from the bottom up at Layer 1. First you must control physical access to a network, then you concern yourself with data security. Expensive and complex software solutions don't do you any good if your network hardware isn't properly secured in the first place. The week after you buy that fancy firewall, your sensitive data could go strolling out the door in someone's pocket.

Why physical access to computers is a problem

Unrestricted physical access to a computer or a network is your number one security threat. If a hacker has physical access to your network, stealing information is easy—the fastest way into a network is not through the firewall, but through a USB port on an unattended workstation. The most dangerous information thief may not be a faraway hacker, but one of the cleaning staff inside your building.

There is virtually no end to ways people with malicious intent can damage your equipment or steal data if they have simple physical access. For instance, they could:

- Damage your equipment using the simple smash-and-kick method.
- Use a tiny USB flash drive to steal data or insert a harmful virus.
- Steal or copy a hard drive and take it away to examine at their leisure.
- Install unauthorised software.
- Boot a computer from a floppy disk and reformat the hard drive.
- Override password protection on a computer by opening the case and replacing the BIOS chip.
- Install a hardware keyboard logger to capture every keystroke you make.
- Learn passwords from sticky notes left near computers or by simply watching people enter their passwords.
- Retrieve papers containing sensitive data out of the trash.
- Use a handheld device such as an iPod®, mobile phone, or digital camera to suck data out of your system.
- Install a network tap and capture data going across your network.
- Run a program to learn passwords or to insert new passwords into your system.

Lock it up!

Before you install that incredible firewall, remember that a simple physical lock is your first line of defence against unwanted network access. Lock up wiring closets, offices, desktop CPUs—anything that could provide physical network access.

Door locks

The first thing you should do to secure your network is to put equipment behind a securely locked door. Server rooms, data centres, and wiring closets should be securely locked as a matter of course. Equipment located in office areas should be kept in a locked cabinet. And, if practical, access to the entire building should be controlled.

Door locks fall mainly into two categories—the old-fashioned mechanical lock and electronic locks.

Even though mechanical locks are simple, straightforward to use, and often difficult to pick, they usually aren't the first choice for door locks in equipment areas. Keys can be lost or stolen and many keys can be easily duplicated at the local hardware store. The key-and-lock combination is somewhat limited because it's secure only if you can keep tight control over the keys.

Additionally, unlike electronic locking systems, mechanical locks and keys don't generate audit trails, so you don't know who had access to your equipment and when they were there.

Electronic access systems using cards, tokens, or biometrics are the most popular door-lock systems for securing IT areas. An electronic access system tracks each user individually and creates a log showing who gained or requested access to the room. Additionally, these systems enable you to customise access, so that each person can enter different areas within your facility.

Cards can be activated and deactivated quickly, so lost cards aren't a problem. A weakness in the system, however, is that of cards which are lost or "borrowed" and used before they can be discovered and deactivated.

The most secure kind of door lock, by far, is the biometric access system. Biometrics is a technology that measures physiological characteristics, such as fingerprints, irises, voices, faces, and hands, for authentication purposes.

Biometric authentication is becoming a popular way to ID people for security purposes because it has the advantage of being both more convenient and more secure than traditional card readers—no one forgets their finger at home or swipes an unauthorised retina.

Biometric devices consist of:

- A reader or scanning device
- Software to convert the scanned data into digital form and compare it to a database
- A database that stores data for comparison

An example of a Biometric Lock System: Black Box Intelli-Pass™ Biometric Access Control (SAC510NA).

Biometric data is encrypted after it's gathered. When a body part is scanned, the software identifies specific data points and converts them to a numerical value using a set algorithm. Then the software compares this value with a number stored in the data base to approve or deny access. Because the database stores a numerical value rather than an actual fingerprint or iris scan, a biometric system does not create privacy issues.

Biometric authentication can be used alone but, to increase security, it's frequently combined with other access control methods such as card readers, pass codes, or digital signatures.

It's worth remembering when you plan your door locks, that a fancy lock system isn't going to do you any good if it's on a flimsy door. Look over the doors to make sure they can't be easily kicked in or jimmied. Be sure you use a latch guard—a simple plate that covers the gap between the door and the jam—to block access to the latch mechanism so the lock can't be popped with a knife, credit card, or screwdriver.

Locking cabinets

With networks now routinely installed in small organisations and the decentralisation of networking, it's now common to find servers and other network equipment outside the traditional data centre environment.

When equipment is installed outside of a locked data centre, it's more vulnerable, not just to hackers, but to every curious passerby who wants to take a poke at it.

Network equipment outside of locked data centres should be housed in a fully enclosed locking cabinet. Cabinets usually feature standard 19" rails for rackmount equipment and are available in sizes ranging from full-sized cabinets to small wallmount cabinets. Cabinets are even available with climate-control features, so you can put them nearly anywhere without worrying about high temperatures and humidity damaging your equipment.

An example of a wallmount equipment cabinet with climate control: Black Box ClimateCab NEMA 12 Wallmount Cabinet with Air Conditioning (RMW5110AC).

Although cabinets usually lock with standard key locks that have associated vulnerabilities, they're increasingly also available with combination and biometric locks.

Laptop computers

Laptop computers deserve special consideration because their small size and portability makes them extremely vulnerable to loss and theft. A stolen laptop can not only divulge sensitive information, it can also provide a hacker with a convenient, direct link into your network.

The best way to prevent a security compromise through a laptop is, of course, to never to have sensitive data or network access on a laptop. Because this isn't always possible, it's wise take extra precautions with laptops.

An example of a laptop lockbox: Black Box Laptop Cabinet (RM415A).

Physically locking down a laptop computer can go a long way towards discouraging a casual thief. Many of today's laptop computers feature a Universal Security Slot (USS), which allows them to be secured to an immovable object with a cable lock.

Many laptop thefts happen in the office. Either use your laptop with a docking station that can lock the laptop securely in place or lock your laptop in a secure desk, cabinet, or specially designed laptop lockbox.

Label your computer. When you physically engrave or tag a laptop computer with identification, you greatly increase your chances of having it returned to you if it's lost and also make it a far less attractive target for theft. It's also important to remember to register the laptop with the manufacturer when you buy it. This enables it to be traced by serial number.

Use BIOS-level encryption to lock your laptop. When a laptop is protected at the BIOS level, a password prompt appears after you start up the laptop but before the system loads and grants access to the computer. Password-protecting a laptop computer isn't going to defeat a skilled hacker who can work on your stolen laptop at his leisure, but it can go a long way towards discouraging the less talented and persistent. Make sure the password locks the hard drive, too, so it can't simply be removed and installed in another computer.

Teach your laptop to call home. Many companies offer tracking software that has your laptop check in periodically and report its position using some combination of a global positioning system (GPS), Wi-Fi® hotspots, a wired Ethernet connection, or a cellular network. This service can help you quickly recover a lost or stolen laptop. Many of these services also enable you to remotely delete data on a laptop if it disappears with sensitive information on it.

CPUs, too

Imagine a waiting room with a video screen on the wall delivering information about flu shots and the value of regular cholesterol checks. A quick check shows that the video is coming from a networked PC under an end table—bonanza for any enterprising hacker.

Computers in public or semi-public areas such as lobbies or waiting rooms are easy targets vulnerable to hacking or just plain vandalism. Either lock these computers up in a secure cabinet or move them to a secure area and use a KVM extender to connect a keyboard, monitor, and mouse placed in the public area.

Security cameras

Because there's no substitute for actually seeing what's going on, video surveillance is a key part of any organisation's physical security plan. With video, you can see exactly what happened to that server and whether the person who did it matches the access card that opened the server room.

Today's digital video surveillance systems are lightweight, inexpensive, and integrate easily into your network. They provide much higher quality video than older systems that recorded to tape and, because they record to DVR rather than video tape, there's no worry about changing or storing tapes. Plus, video systems integrated into your network can be accessed from anywhere in the network—even across the Internet.

Today's video systems are smart, too. You can set them to record continuously, record only when a door is opened, record on a pre-set schedule, or record in response to a motion detector. Many systems can forward alarms and images to an e-mail account or even to your smart phone.

A long-range wireless IP camera: Black Box LongSpan Security Camera Housing Kit (LS900-DOME-KIT) with Sony IPELA 340° P/T/Z IP Camera (SNC-RZ50N).

To secure areas without convenient network connections, consider a 802.11g wireless camera, which can link to your wireless access point. For longer-range applications, a 900-MHz wireless Ethernet extender can be an effective way to reach across long distances.

Finally, remember that a surveillance camera doesn't necessarily have to connected, or even be real, to be effective. A strategically placed "dummy" camera can discourage trouble by making people believe they're being watched.

Secure your in/out devices

A networked PC holding secure data should have all avenues in and out secured. This includes ports, drives, and attached devices such as keyboards.

USB ports

The common USB port is, hands down, one of the easiest portals to bypass the network to get data in and out of a computer. USB ports are ubiquitous—every desktop and laptop computer has at least one—and easy to use. Compact USB flash drives are inexpensive, fast, and can easily hold 8 GB or more of data.

In only a few minutes, a hacker can pull a flash drive out of his pocket, "slurp" all the data off your computer, and you'll never know it happened. An iPod® can also be used for this, but that's not as common because an iPod is more expensive, more easily traced to its owner, and more difficult to program.

Another way a hacker can get into your system is to load his/her software tools onto a flash drive and leave it laying around in a public area such as the smoking area. A curious finder will invariably plug the flash drive into a computer's USB port to see what's on it. Then the software on the flash drive launches itself and the hacker is in.

A common problem with USB ports is that people will use them to install unauthorised software on a computer. Not only can unregulated software cause system problems, but organisations are required by law to purchase software licenses for any application on their computers—even if they don't know about it.

Fortunately, you can buy inexpensive and effective port locks to keep USB ports from being used. These locks can be overcome, but they go a long way toward slowing down access to the port.

You can also disable USB at the BIOS level. This can be reversed, but it has the disadvantage of being an all-or-nothing proposition—it takes out all the USB ports, so you can't use USB keyboards, mice, or printers.

Other in/out ports and drives

Although USB ports are the most common way to break into a computer, don't forget that other serial and parallel ports can also be used to get at a computer. They aren't quite as easy to use as a USB port, so they present less of a threat, but that doesn't mean they're totally harmless. Fortunately, they're also not used much today and can usually be totally removed from a computer or disabled without being missed.

Limit CD, DVD, and floppy drives. In today's networked age, it's easy to forget that data can still travel in and out of a PC on a disk and that this can be a prime conduit for installing illicit software. Ideally, a secure PC has no removable-media drives built into it. If you do have drives and wish to secure them, physical locks for CD, DVD, and floppy drives tend to be ineffective, so it's usually preferable to use software that requires a password to make the drive accessible.

Keyboard loggers

A keyboard logger is a readily available, insidious, little spy device that installs between a keyboard and a CPU and records every keystroke made on that keyboard for up to two million keystrokes—a year of typing for most people. A keyboard logger records everything you type, including passwords.

A keyboard logger is unobtrusive and looks like an ordinary dongle or maybe a surge protector. It requires no skill to install and, because it uses no system resources, it's undetectable except by physically looking for it behind the computer. Also, make sure that the keyboards used in your organisation are the same as the keyboards issued, because keyboard loggers exist that are built right into keyboards.

Consider banning handheld electronic devices

They're popular and your staff will hate you if you ban them, but the fact is that many of today's small electronic devices such as iPod MP3 players, mobile phones, digital cameras, and PDAs contain a vast amount of memory and can be adapted to suck data out of a computer right through a USB port. Because an iPod is so often used, the general name for this activity is podslurping.

If you have very sensitive data on your computers and are extremely concerned about security breaches, banning these handheld devices is definitely something to consider in your security plan.

Use fibre optic cable

Wherever security is a concern, choose fibre cable over copper. Fibre doesn't radiate signals and is extremely difficult to tap. If the cable is tapped, it's easy to discover because the cable leaks light, causing the entire system to fail. If an attempt is made to break the security of your fibre system, you'll know it.

Fibre has other benefits, too, that make its installation worthwhile. Because it's immune to EMI/RFI interference, you can install it in electrically "noisy" areas. Plus, fibre supports higher bandwidths and longer distances than copper does.

Protect data

Separate secure networks and unsecure networks

Today, it's taken for granted that any organisation's internal network is connected to the Internet. But even with the most capable firewall, an Internet connection is never entirely secure.

If your network contains very sensitive information such as patient records, corporate financial data, or the latest plans for a stealth bomber, one of the most effective things you can do to maintain privacy is to physically separate it from the Internet. Of course, your users are probably still going to require Internet access and you can provide it to them, just not on the same network that contains sensitive data.

The most obvious way for one person to access both a secure and an unsecure network such as the Internet is for them to have a separate computer for each network. This solution tends to be expensive, but it's ultimately a very secure solution because sensitive data is never on the computer that accesses the Internet.

An example of a KVM switch: Black Box ServSwitch™ Secure (SW4007A).

A convenient way to have two separate CPUs at the desktop without also having two separate monitors, keyboards, and mice, is to use a KVM switch to switch between the CPUs. Because a KVM switch keeps the CPUs entirely separated, it's impossible for a user to transfer information from one to the other. For particularly sensitive installations, choose a secure KVM switch, which is specially shielded so there is not even the remotest chance that an electrical signal can leak from one CPU to the other.

Another solution for accessing two separate networks is to have a manual switch to enable a single computer to access two different networks in turn. You can use either a copper or a fibre switch, but fibre is generally regarded as more secure (if you need this level of security, you should be using fibre anyway).

An example of a manual network switch: Black Box Fibre Optic AB Switch (SW1002A).

This solution isn't quite as secure as having separate CPUs for each network because of the danger that a user will leave a sensitive file on his/her desktop while accessing the Internet.

Keep sensitive data off laptops and other portable devices

It makes the news with some regularity—a laptop containing sensitive information is lost or stolen, spilling the personal data from thousands, even millions of people. You'd think with a story like this making the news once or twice a week, organisations would get wise and keep sensitive data off laptop computers.

Yes, you can encrypt laptops and equip them with chain locks, but the fact is, these portable devices are meant to travel and they often get lost or stolen. They get left in cabs, snatched from hotel rooms, and generally disappear.

Make it a policy to minimise sensitive data allowed on laptop computers, by allowing it only when absolutely necessary and limiting it to the least amount of information that will get the job done. Make sure that data is well encrypted and removed as soon as it's not needed anymore.

Don't forget that many other portable devices such as phones and PDAs are also computers in their own rights and can carry sensitive data.

Data backup

No matter what precautions you take against equipment damage, accidents do happen—power surges, spills, drops, etc.. It's impossible to guard against every possible scenario. Equipment can be replaced; data can't be. Have a comprehensive plan for backing up and archiving data.

Protect equipment from accidental damage

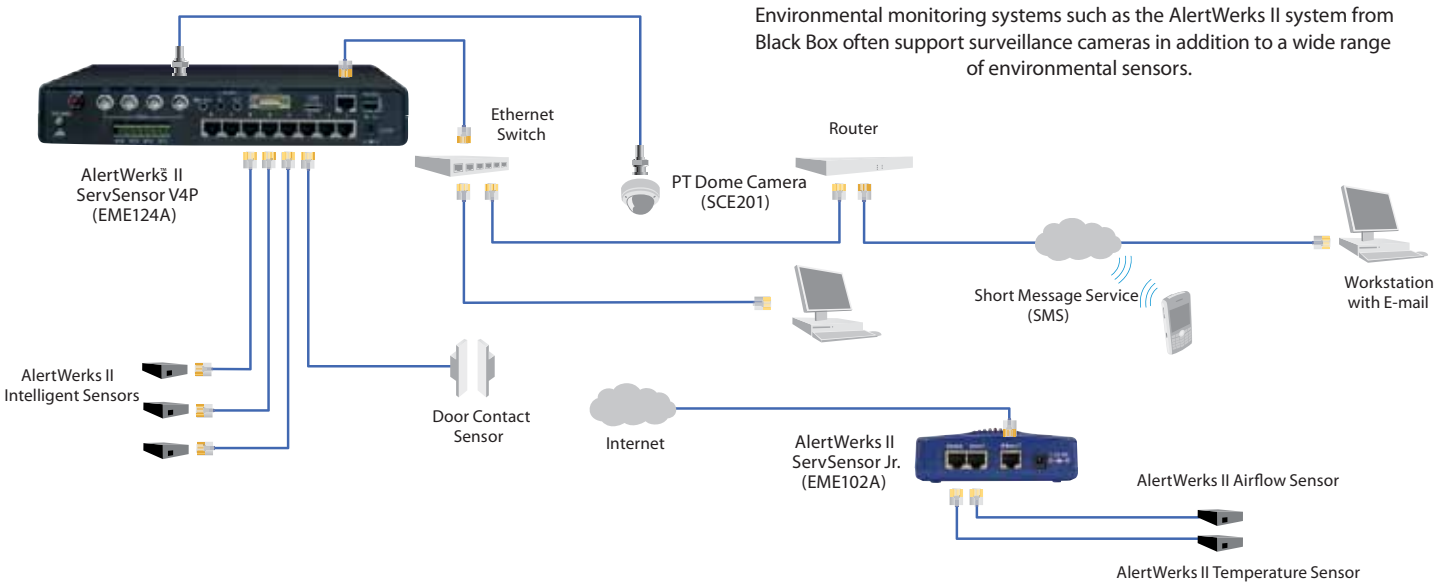
Network security means not just protecting the network against deliberate, malicious damage, but also protecting it from accidental damage from environmental factors such as heat, humidity, smoke, and power surges.

Environmental monitoring

Network devices can be taken out as easily by high temperatures as by a hacker. Part of the job of protecting your physical network is to ensure that network devices are always kept in a safe, well-regulated environment. Environmental factors are of special concern when equipment is installed in remote, unsupervised locations.

Environmental monitoring products enable you to actively monitor the conditions in your rack, server room, data centre, or anywhere else you need to protect critical assets. Conditions monitored include extreme temperatures, humidity, power spikes and surges, water leaks, smoke, and chemical materials. With proper environmental monitoring, you're alerted to any conditions that could have an adverse effect on your mission-critical equipment. Environmental monitoring products can also alert you to potential damage from human error, hacking, or prying fingers. Many systems can be combined with video monitoring so you can keep an eye on your equipment as well as monitor conditions.

Environmental monitors consist of three main elements: a base unit, probes or sensors, and network connectivity and integration. The base units may contain one or more built-in sensors, as well as ports for hooking up external probes. Additionally, they include an Ethernet port and have software for remote configuration and graphing. This software may also work with existing network management software, such as SNMP systems.



Surge and power protection

Networking devices generally require a steady, uninterrupted supply of 230 volts alternating current (VAC). In the UK, this is the standard power provided by local public utilities. This electricity is generally affordable, clean, and reliable, but it is subject to fluctuations. Too much voltage (surges and spikes) or too little voltage (brownouts and power outages) can damage your equipment or render it temporarily unusable.

Surge protectors are devices designed to protect your equipment from overvoltages that can damage your delicate electronic equipment. Surge protectors should be installed both on power lines and data lines.

An example of a data-line surge protector: Black Box CAT5 100BASE-TX Surge Protector (SP251A-R2).

Practically speaking, surge protectors don't absorb or otherwise diminish damaging power surges. Their primary function is to divert these destructive forces away from your sensitive circuitry. In the face of an extremely large surge, a surge protector will break the link to your hardware. Ultimately, surge protectors are designed to fail, sacrificing themselves to protect electronic devices.

A surge protector guards against too much power, but many power problems show up as brownouts (low voltage) or blackouts (complete outages), which can render your equipment ineffective or totally inoperable. An uninterruptible power supply (UPS) protects your systems against conditions of too little power.

Having a server down can bring your operation to a halt. Although the loss of a single switch or router may not bring an entire organisation to a standstill, it can result in zero productivity for entire workgroups or remote offices.

An example of a UPS: APC Smart-UPS XL (SUA3000RMXL3U).

For a small fraction of the cost of your networking hardware, you can purchase a UPS to protect your network from brownouts, blackouts, and surges. It keeps power flowing, giving you enough time to shut down safely during a power outage. It also regulates your power, smoothing out dangerous overvoltages and undervoltages, spikes, surges, and impulses that often go unnoticed.

Treat wireless with care

Wireless is, by its very nature, unsecure. A cable-based network requires access to a cable or a port to get into a network, but a wireless network spreads its cloud far and wide for anyone with a laptop computer or a PDA to tap into.

Yes, there are encryption standards but, the truth is, basic WEP encryption is only marginally better than no security at all, and tools to crack the more advanced WPA and WPA2 are readily available. Using encryption to protect your wireless network will keep out the casual browser, but it won't do much to stop someone determined to get into your network.

The only really secure way to use wireless is to use it only within areas you have total physical control over. In particular, watch that your wireless signal doesn't spill over into a public or semi-public area such as a sidewalk or building lobby.

Also be aware of unauthorised access points that your users have plugged into your Ethernet network for their own convenience. Unauthorised access points range from a mere nuisance to a real security threat in a large network. Because it's so easy for users to plug in an access point, you have to constantly guard against it. Just one unsecured access point can be a vulnerable entry point for an entire network.

Don't forget the paper trail

Computers produce paper. Lots of paper. Those piles of printouts discarded into the recycling bin are prime fodder for an ambitious dumpster diver. If you don't want it seen, shred it.

The most vulnerable security gap—humans

No amount of securing your network is going to do you any good if the people in your organisation cheerfully hold doors open for perfect strangers, plug in random unauthorised devices, and have their passwords written on post-it notes on their computer monitors.

A complete security plan includes educating your staff to be aware of physical security issues—in this arena, you want them to be vigilant and somewhat paranoid.

In conclusion

Physical network security is as important or more important than software-based security—a failure in physical security can quickly nullify all the work done on the software side to secure your network. However, this aspect of security is often overlooked or poorly planned. A solid network security plan, includes a thorough review of physical security, including access control, surveillance, data centre monitoring, and data backup.

About Black Box

Black Box Network Services is a leading network solutions provider, serving 175,000 clients in 141 countries with 192 offices throughout the world. The Black Box catalogue and Web site offer more than 118,000 products including biometrics, remote access solutions, cabinets, fibre optic cable, and environmental monitoring. Its comprehensive environmental-monitoring solution, AlertWerks II, guards mission-critical IT equipment against physical threats from temperature extremes to water damage, and it offers a video option, too.

Black Box also offers a complete range of networking products including switches and converters, as well as cabinets, racks, cables, connectors, and other video, audio, and data infrastructure products.

Black Box is known as the world's largest technical services company dedicated to designing, building, and maintaining today's complicated data and voice infrastructure systems.