OFFICE SECURITY ISSUES: RISKS, CONSIDERATIONS, AND RECOMMENDATIONS

Sean P. Logue

ABSTRACT

This document examines the current state of computer security in the office, and offers information and recommendations on various security solutions.

ITIRC KEYWORDS

- Office computer security
- Securing workstations and desktop computers
- Security considerations for computers in offices and workspaces

ABOUT THE AUTHOR

Sean has over fourteen years of experience in the technical writing, development, and testing fields working for a large computer company. He currently manages a combined Test and ID department.

CONTENTS

OFFICE SECURITY ISSUES: RISKS, CONSIDERATIONS, AND RECOMMENDATIONS

Due to the now common use of computers in business settings, there is often sensitive data stored on disk, tape, or sent over the Internet or phone lines. This data is generally easily accessible and unprotected.

There is a bewildering array of security devices designed to do anything from user verification to simply stopping someone from walking out of the office with a graphics card under his arm. While this allows great freedom of choice, it also makes the choice a complex one. In addition, if not enough is done, or if the system is incorrectly installed, the results can be worse than if nothing was done at all. For example, the wiring for a system that detects open doors needs to be shielded and separated from the main electrical wiring of the building. If it is not, the system may be easily bypassed, or may not work at all. In this situation, the system hinders only the innocent user.

The best way to decide what is best for a company or home PC is to first identify how much and what type of security is needed. Is it necessary to keep track of who uses the PC and at what times? Is the data sensitive enough to protect or is the main object to prevent the theft of the computer itself? This type of question needs to be answered before a single purchase is made.

PHYSICAL SECURITY

The first category of security systems is the physical one. These are the devices that are intended to protect the computer system itself. Some may also have the added benefit of preventing unauthorized computer use while the office is closed. The most obvious of these is the lock on the office door. It affords a measure of protection as long as it is used.

Other devices are available as add-on products. There are thin cables available that loop through plates attached to the base unit and monitor by space-age adhesives. The cables are held together with either a combination or key lock. This arrangement is relatively inexpensive, costing from $35 to 200 dollars depending on the system, and works well. Also, these systems can be installed by anyone, eliminating costly and time consuming professional installation. The main problem is psychological in nature. Some users may not like their PC's to have locks and chains hanging off of them. For this very reason, most of the products try to keep a low profile.

Another idea is removable hard disks. In many cases, a hard drive used in a business contains a great deal of sensitive information such as employee data or copies of letters. When using a removable hard disk, at the end of the day the disk can be removed and placed in a safe or even carried home. These systems are not much more expensive than regular hard disks and have been around long enough to prove their reliability.

BIOMETRICS

For installations with much greater security needs, an entire field of study, called biometrics, is available. A biometric device is something that verifies someone based upon his or her individual physical characteristics such as fingerprints, retinas, hand geometry, wrist veins, voice analysis and signature analysis. These systems have inherent advantages over more conventional systems that use a key or magnetic card because physical characteristics can not be stolen or "loaned" to a friend. In the future most companies will use one or more forms of biometric devices, perhaps in combination with other systems.

Most biometric systems rely on the well-known idea that each person has individual fingerprints. By placing one hand on a small optical plate, a scanner can "read" the finger prints and compare them with the ones on file. If they match, the person is admitted. These systems are currently the most popular of all biometric devices, but critics are quick to point out the problems with smudged or dirty plates, cuts and calluses.

Another device is the retinal scan. Like fingerprints, each person has a unique pattern of blood vessels on the inside of the eye. The person looks inside an eyepiece while a low-level infrared light scans the portion of the eye that contains the greatest number of vessels, comparing them with previously obtained patterns. The whole process takes about two seconds. Although the level of light used is far below current health standards there are some concerns about damage to the eye resulting from the light. The cost may also be prohibitive, depending on the level of installation required.

To prevent unauthorized access to a computer connected to phone lines is another problem. The physical approach is the use of special hardware called a callback modem. It works by answering the phone, then allowing the user to type in a name and usually a password. The modem then looks up the user in its memory and calls the phone number belonging to that person. In this way, the person called knows when his password has been compromised because the computer will call him when he hasn't called it. Additionally, the person who used his name was never allowed to interface with the computer at all; the modem allows computer access only to the people it calls.

This technique sounds absolutely fail safe. Unfortunately, it is also a very good example of how false confidence can lead to a mistaken sense of security. These systems were in use about six months before some determined people tried sending a dial tone down the telephone line just before the modem hung up. The modem, thinking the line was disconnected, dialed the appropriate number (which, of course, did nothing as the line was still open), and allowed the person access. Now, of course, this defect is known by the manufacturers and is provided for. Still, it should be remembered that no system is absolutely secure against determined criminals.

SOFT SECURITY

The "soft" approach to prevent both direct computer access and access through phone lines is widely used. This approach attempts to prevent the use of unauthorized information by system software rather than by hardware. Currently, this category consists mainly of passwords and data encryption.

PASSWORDS

The use of passwords is an old practice that dates back almost from the first large computers. The concept is a simple one. The user enters a name then a password. The system software then compares the name and password against an internal list. If they match, the person is granted access.

Many variations are used with the password to provide an extra measure of data security. Some systems will lock up for a set amount of time after a certain number of incorrect passwords are entered. This helps stop someone from having a computer guess all possible password combinations. Also, almost all will keep what is known as an "audit trail" of use. This is a list of who is on and at what times. By examining the list, operators may be able to spot discrepancies in computer use that may indicate a compromised password. Computer use by an employee who is on vacation, for example.

In a password protected system it is important that all users change their passwords often and tell them to no one. In fact, changing passwords is so important that some systems will enforce it. They keep track of how long the current password has been in use, and when it "expires" they will require a new one. Also, it is important to use enough characters to eliminate the chance of password guessing. Three characters is not enough. Seven is about average. Security of password based systems relies heavily on user cooperation.

DATA ENCRYPTION STANDARD (DES)

Data encryption is a last chance attempt at stopping information from getting out to unauthorized people. After the person has gotten past both the physical systems and the soft systems, data encryption ensures that he or she will still not be able to read the information. Like the other security systems, there are numerous data encryption standards available. The current favorite is the "data encryption standard" or DES.

DES is a government supported standard which means that it is used by federal agencies to encode sensitive information. It was originally developed at IBM under the code name Lucifer and would take years to decrypt using very expensive, specialized super computers. Although the standard is specified for hardware, many software implementations are available. The software is less expensive, but is much slower and is vulnerable to a knowledgeable programmer who could modify the code.

One of the reasons DES is so effective is that it utilizes an algorithm known as cipher-block chaining. This means that even if some of the text is known, such as the first paragraph, the rest of the document cannot be decrypted. The cost of these systems ranges from $50 for software to about six hundred dollars for hardware. As with the password based systems described earlier, care must be taken in selecting a password. Also, if it is lost or forgotten, valuable data could be lost forever.

SUMMARY

The most important considerations when setting up data security are how much security is needed and at what cost. Setting up a fortress when only a small lock is necessary will hinder valid computer use as well as being expensive. Too little security will leave data open to attack and perusal. And remember: no system is totally secure, some are just more secure than others.