

CYBER-CRIMINALS AND DATA SANITIZATION:

A ROLE FOR FORENSIC ACCOUNTANTS



By Dale L. Lunsford, PhD, and Walter A. Robbins, DBA, CPA, Cr.FA

Key Words: cyber-criminal, disk sanitization, disk wiping, discarded computers, retired computers

Abstract

Forensic accountants are typically involved in fraud prevention/detection. However, their expertise may also be needed to protect sensitive/confidential information that may become accessible through an organization's discarded computers. Cyber-criminals (CCs) acquire old discarded computers with the intention of collecting sensitive/confidential information for illegal purposes. Deleted files, recovery partitions, configuration files, password storage, and special hardware devices are areas targeted by CCs. Forensic accountants should be aware of this potential danger and understand that the process of sanitization, if followed correctly, can prevent future users of retired computers from gaining access to sensitive/confidential information.

This article is approved by the following for continuing education credit:



ACFEI provides this continuing education credit for **Diplomates**.

ACFEI provides this continuing education credit for **Certified Forensic Accountants**.

ACFEI provides this continuing education credit for those **Certified in Homeland Security**.

Introduction

While forensic accountants are typically involved in fraud prevention/detection, another area where their expertise may be needed is in the protection of sensitive/confidential information that may become accessible through an organization's discarded computers. The reality of this potential danger was highlighted in 2002, when the U.S. Veterans Administration Medical Center in Indianapolis discarded 140 desktop computers, many of which were sold on the open market. It was later discovered that several of these computers' hard drives contained sensitive medical and financial information, including active government credit card numbers and information identifying patients diagnosed with AIDS and mental health problems.¹

Most people believe that by deleting files, information will be permanently removed from discarded computer equipment. This belief is dangerous and simply untrue. Consequently, forensic accountants can provide a valuable service to organizations that retire old computer systems by advising clients regarding the inherent risks and outlining the steps necessary to ensure the confidentiality of information stored on the discarded equipment.

Areas of Hidden Data

CCs usually look for information in five areas of a computer: deleted files, recovery partitions, configuration files, password storage, and special hardware devices.

Deleted files. When disposing of an old computer, the user often deletes all documents containing confidential information and empties the recycle bin, believing this process erases the files. However, delete/erase commands do not actually remove a file's information from the hard disk. Instead they rewrite the metadata that pointed to the file, leaving the disk blocks containing the file's contents intact. Thus, such information is still vulnerable to cyber theft.

Usually, a CC will simply use file recovery software to undelete files and then examine the contents for confidential

information. Even if the computer user has reformatted the disk or removed the drive partitions, the CC can use un-formatting and partition-recovery software to recover data. These programs are inexpensive and easy to use; in some cases, free trial versions are available on the Internet. As a result, even an amateur can search a used computer and easily recover confidential files.

In addition to user-maintained files, confidential data may also exist in cached files and application-generated backup files. Normally, users are unaware of and do not delete these files when retiring old computers. File caches are located in operating system (OS) directories or hidden locations (to prevent users from accidentally deleting them). Computer users are usually not aware that many application programs store back-up files in the same directories where the applications are located. Unfortunately, most CCs know exactly where applications put such back-up files and can copy and search them for useful information.

Recovery partitions. Personal computer OSs organize a hard disk into one or more logical sections called partitions. This allows the user to have multiple OSs on the same hard disk or create the appearance of having multiple hard disks. Some data recovery tools, such as IBM Rapid Restore, Farstone RestoreIt!, and Altiris Local Recovery, use hidden partitions to store a backup copy of personal files and to protect these files from unexpected computer disasters that might otherwise lead to data loss. These products enable quick local data recovery. Because these recovery partitions are generally hidden from the user, users may forget to delete the backup copies of files, allowing a future user to gain access to unauthorized information.

Configuration files. Any software purchased today will include a number of configuration options that determine how the software works, which features are available, and other information intended to simplify the user's life. Starting with Microsoft Windows 95, all OSs' configuration information is consolidated

and stored in one central database called the registry. Also, application-specific initialization files maintain information about the configuration of each associated application program. Microsoft encourages application developers to use the registry to store their individual program's configuration information. The registry organizes configuration information hierarchically, with actual settings at the lowest levels of the hierarchy stored as name and value pairs. Ideally, by centralizing this information in one database, configuration settings common to all applications need only be stored once, the installation of applications will be simplified, and the overall system will be more stable.

Unfortunately, the registry and initialization files provide substantial details about the configuration of the hardware, the OS, and applications on the computer. The registry also contains a number of most recently used lists showing files opened by various applications, as well as the location of application files and network resources accessed by the user. Consequently, these files serve as a rich source of useful information. If a CC wants to recover data on a retired computer, knowing the file locations used by various applications simplifies the task of recovery. Perhaps more importantly, information in the registry and initialization files can be of great value to a CC wishing to misuse a company's network resources. For instance, the configuration files can provide information about the security measures employed by the company and the organization of files on servers.

Passwords. Many users become overwhelmed trying to remember all of the login identification and passwords needed to access e-mail, applications, databases, and web sites. In an attempt to reduce this problem, some versions of Microsoft Windows and many other programs, including e-mail software and web browsers, provide the capability to store login identification and passwords so that the user does not need to remember these identifiers.

Often the OS or applications store identifiers and password data in the OS's registry or application-specific configura-

tion files. Ideally, the application encrypts the password so that it is not easily accessible; however, developers often do not use strong encryption techniques to protect the passwords. If the encryption technique used is weak, or the user selects a poor password, then password recovery or cracking software can determine the password and provide such information to the CC.

In the case of popular applications, sometimes a user develops a password recovery program and distributes the program on the Internet as a service to the user community. Unfortunately, CCs can also use this utility. Even worse, some applications automatically log users in if the user tells the application to remember the password. Popular web browsers offer to remember passwords to web sites, which can include the password to the company's local area network. In these cases, the CC is not required to spend any time cracking the password.

Special hardware devices. Computer hardware can provide a CC with important information about the network architecture and security measures used by the company discarding the equipment. For example, the presence of a wireless network card tells the CC that the prior user accessed a wireless network. Thus, the criminal will look for configuration information related to the wireless network, including the network name and the encryption keys it uses. Also, the presence of network code identification and authentication hardware may alert the CC to special security measures employed by a company. Moreover, the CC may move the hardware device to a computer that will be used in an attack on the company's information system.

Safety Measures and Their Implementation

The forensic accountant should understand the process to follow to prevent future users of retired computer systems from gaining access to sensitive/confidential information, as well as information about the network architecture and company security measures. The four-step

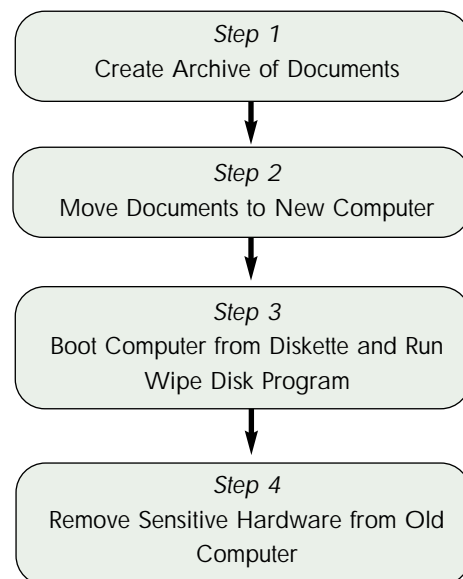
procedure, known as sanitization, should be followed each time a computer is retired from service. The focus of this process is on wiping all information from the disk drives in the old computer and removing any sensitive hardware. Figure 1 illustrates the sequential steps in the sanitization process.

Step 1: Create Archive of Documents

The first step in the sanitization process is to make a backup copy of all data files contained on the computer, a difficult task due to the way applications store data. By default, most Microsoft applications store files in a directory called My Documents. Other applications may use Microsoft's My Documents directory, create their own directories, or even save new files to the location where the applications' installations are located. Tracking these diversely located files can be challenging; as a result, it is best to use a disk-imaging tool to make a copy of all files on a high-capacity removable disk (e.g., an Iomega Zip disk), compact disk (CD), digital versatile disk (DVD), or high-capacity external drive. Applications for performing this task include Norton Ghost, Paragon Drive Backup, NovaStor Instant Recovery, and Acronis True Image, as well as other commercial, shareware, and freeware products.

It is also suggested that when moving to a new computer it is a good time to reorganize files. One approach is to consolidate the files in one location and point the applications to this location. While this is a good practice, remember that using Microsoft's My Documents directory can be risky, since some computer viruses focus on this directory during attacks. One way to minimize this risk is to use a different directory to store personal documents (e.g., a directory called "My Stuff"). Simply point each application to the directory you designate for your documents, be it My Documents or some other location. Within this directory, you may have created subdirectories based on whatever organizational scheme you find appropriate. A good practice is

Figure 1. The Four-Step Sanitization Process



to organize your files on your computer in a manner similar to the way you organize paper documents.

Step 2: Transfer Documents

After the backup process is complete, all files need to be copied to the new computer. This activity is presented as step 2 in Figure 1. There are software packages that make this process rather easy. For instance, IntelliMover, created by Detto Technologies, provides the software and data transfer cables (either USB or parallel) necessary to transfer all computer settings and data along with personal files and folders. Once the copy process is finished, it is necessary to delete all files from the old computer, including operating system files, so that there is no information about application settings, passwords, or other encryption keys. However, just deleting these files is not sufficient. The computer drive must next be sanitized.

Step 3: Sanitization

Sanitization, represented as step 3 in Figure 1, is the process of wiping clean all data stored on a computer hard drive. There are three methods for sanitizing a computer: disk shredding, disk degaussing, and disk wiping.

Disk shredding: Disk shredding is the

process of physically shredding a disk, similar to shredding paper, so that the disk hardware is no longer usable. This method provides the most secure means of destroying data on a disk. The primary disadvantages of this method are that a technician must remove the disk from the computer, special equipment is required to actually shred the disk, and the ability to transfer the computer to a new user is limited because the computer no longer has a hard disk.

Disk degaussing: Disk degaussing is the process of exposing the disk to strong magnetic fields to destroy the data on the disk. This method provides a high level of security by eliminating any residual magnetic data on the disk. The primary disadvantages of this method are that a technician must disassemble the disk before degaussing, and the manufacturer must reformat the disk before reuse. Also, special equipment is required to degauss a disk, and the degaussing equipment can damage or destroy other components if improperly used or stored.

Disk wiping: The final method, disk wiping, applies a four-step process to each addressable location on it. The steps consist of writing a character, writing the character's binary complement, writing a random character to the addressable location, and then verifying the last write. This process results in filling every addressable memory block. The primary disadvantages of this method are that it requires special software and is generally not appropriate for top-secret information. Fortunately, the software is inexpensive, generally in the \$25 to \$50 price range, and most users do not store top-secret information, so this method is sufficient for most confidential data and can be performed by the user before transferring the computer to the information systems department.

A number of products exist to wipe the contents of a disk, including KillDisk (Active), Disk Wiper (Paragon), BCWipe (Jetico), CyberScrub (CyberScrub), WipeDrive (WhiteCanyon Software), Ghost (Symantec), Wipe Info (Norton), and 12-Shredder (SuperGee). Most com-

mercial versions of disk-wiping products comply with U.S. Department of Defense 5220.22-M, which defines data destruction standards for information below the top-secret security level.² Some vendors provide free versions of the software for non-commercial entities. The free versions generally perform a one-pass wipe process, while the commercial versions can perform multiple-pass wipes.

As shown in step 3 of Figure 1, the disk-wipe process consists of two major steps, booting the computer from a diskette or CD and wiping the disk clean. It is important to note that before the disk sanitation process begins, all necessary files must be successfully copied to either a new computer or to a permanent archive. Once a computer has been sanitized, no files can be recovered from it.

Microsoft Windows and other OSs generally do not permit the deletion of critical operating system files. To get around this, you can boot the computer from a diskette. In some cases, the disk-wiping software includes a utility to create a bootable diskette with all of the necessary software. If not, simply put a blank diskette in the diskette drive and use Windows Explorer to format the diskette. Select "Create an MS-DOS start-up disk" so the format process will add the necessary system files to the diskette. After the format process is complete, copy the wipe-disk program to the diskette. The instructions included with the wipe-disk product you select should identify any files that you must copy to the diskette. In most cases, the wipe-disk program is in a small, self-contained executable file so that it will fit on a diskette. You should clearly label the diskette (e.g., "Disk Wiper") so that no one accidentally uses it in a way that leads to undesired data destruction. To sanitize computers without diskette drives, use a wipe-disk program that comes on a CD or that can create a bootable wipe-disk CD; recent releases of commercial disk-wiping software include this capability.

Once you have a boot diskette with the wipe-disk program installed, shut down the computer, place the diskette in the

diskette drive, and restart the computer. Many older computers automatically attempt to boot from the diskette drive if a diskette is in the drive. If the computer loads Microsoft Windows automatically, the computer has booted from the hard disk. In this case, consult the reference material for your computer to see how to change the boot sequence to boot from the diskette drive. Once you have made this change, restart the computer.

After booting from the diskette, run the wipe-disk program. Wipe-disk programs generally are either command- or menu-driven. If the wipe-disk program is command-driven, you must enter the name of the program at the MS-DOS prompt, followed by a series of parameters. The parameters specify the drive to wipe (e.g., C:), the number of times to wipe the drive, and other options. If the wipe-disk program is menu driven, you can specify the same information using menus and text prompts. Some products support both menus and commands so that each user can select his or her preferred method; this is especially useful for information systems departments that want to create diskettes to wipe numerous computers. The time required to wipe a hard disk can vary substantially depending on the age and capacity of the drive.

Step 4: Remove Sensitive Hardware

The end of the process is shown in step 4 of Figure 1. Since the disk-wiping program eradicates all files on the computer, including data files, applications, and OS files, this significantly reduces the likelihood of a CC gaining access to useful information. However, before disposing of the computer, the information systems department should remove any add-in hardware related to the company's local area network and security systems. This denies the CC access to the one remaining source of information about the company's network architecture and security systems.

Case Illustration

In 2003, a colleague's computer was earmarked for retirement. Prior to removing

the computer from service, he transferred all data files to his new computer. He then deleted all files on the old machine using utilities included with Microsoft Windows 2000 Professional. Because he was particularly concerned about unauthorized access to confidential data that might still remain on his old computer, he asked us to examine the machine. We explained that he had not followed appropriate procedures and his old computer was still vulnerable to a CC attack. We applied the following steps to ensure information confidentiality.

First, we logged on to the computer as an administrator. Since we did not know the password for the administrator account, we used a free cracking tool available on the Internet to reset the administrator account's password to a new value and then logged on to the computer. We also set the password of the owner's account to a known value. We now had unrestricted access to the computer. Instead of booting the computer and logging on as we did, we could have installed the hard drive from the target computer in a different computer as a secondary drive and set the drive to a read-only state. This would have given us access to the drive without risking the loss of important data during the boot process. This approach requires a second computer and additional hardware knowledge. Assuming a would-be attacker would have minimal hardware resources available, we opted for the more direct-attack approach.

Next, we ran a commercially available file recovery program (approximately \$30) from a diskette. We used the file recovery program to locate any recoverable data files on the computer. Based on the file names, we identified files that we believed might contain confidential information. We transferred these files to a high-capacity removable disk. We had the computer owner review the files to determine if they contained confidential information; he confirmed that they did. In a live setting, the cracker would have examined the files to identify locations of other useful information; however, to protect

the confidentiality of the information we did not do this.

At this point, we used the sanitization process described earlier to destroy all data on the computer's hard drive. We created a boot diskette, copied the disk-wiping software to the diskette, booted the computer using the diskette, and ran the program to wipe the disk. The software we used can perform the wipe process repeatedly, as specified by the user. We selected the option to perform the wipe process one time. It took approximately 1 hour to wipe the 20-gigabyte hard disk. Since the computer did not contain any sensitive hardware, we did not have to perform the last step of the sanitization process.

To verify that the computer no longer contained any recoverable data files, we attempted to boot it. Since the wipe process removed all operating system files, as expected, the first boot failed. Next, we booted the computer using a boot diskette. We used a partition and file recovery program to scan the computer for any recoverable files. This scan failed to find any partitions, programs, or other files on the disk. Finally, we used a sector editor to search the surface of the disk for any usable data; this search also failed to find any remaining data files. Based on these results, we concluded that the sanitization process had sufficiently sanitized the computer, and as a result we had successfully preserved information confidentiality.

Conclusion

Organizations are coming under increased scrutiny when it comes to privacy and the safeguarding of sensitive/confidential information. Because this information is often stored on personal and company computers, entities must take special precautions when disposing of old computers. Because of their training and skills, forensic accountants are in an excellent position to provide assistance to organizations regarding the security of information on discarded computers. The forensic accountant can ensure that confidential

information is removed from all old computers through the process of sanitization before disposal.

Forensic accountants can also advise organizations about the inherent dangers associated with their confidential information inadvertently being left on old discarded computers and the procedures necessary to ensure the safety of such information. Using a procedure such as sanitization can dramatically reduce the likelihood of a company facing lawsuits, criminal prosecution, or other embarrassing situations.

Notes

1. J. Hasson, "V.A. toughens security after PC disposal blunders." F4 (26 August 2002).
2. Department of Defense (January 1995), *National Industrial Security Program Operating Manual*, retrieved July 1, 2003 from http://www.dss.mil/isec/nispom_0195.htm.

About the Authors



Dale L. Lunsford, PhD, is an associate professor of information systems at High Point University in High Point, North Carolina. He holds a doctorate in information systems management from Ohio State University.

He has published papers examining emerging technologies, ethics, web application development, and computer security.



Walter A. Robbins, DBA, CPA, Cr.FA, earned his doctorate of business administration from the University of Tennessee. He is currently a professor of accountancy at the Culverhouse School of Accountancy at the University of Alabama. His research has appeared in a number of academic and professional journals.

Dr. Robbins also provides litigation support services as a consultant and has worked on a number of civil cases. He is a Certified Forensic Accountant and has been an ACFEI member since 2002.

Earn CE Credit

To earn CE credit, complete the exam for this article on page 66 or complete the exam online at www.acfei.com (select "Online CE").