

# Securing Your Electronic Information Under Sarbanes-Oxley

By

Gregory L. Fordham, CPA, CIA, CCE



***WWW.KNFCON.COM***

1303 Hightower Trail, Suite 315  
Atlanta, GA 30350  
770-642-0311 (voice)  
770-642-9913 (fax)  
greg@knfcon.com

## TABLE OF CONTENTS

Introduction .....	1
Electronic Information When Responding to Whistleblowers .....	2
Data Sources .....	2
Personal Computers and Accessories .....	2
Shared Devices .....	3
Specialty Devices and Application Databases .....	3
Preservation Methods .....	4
Read Only Devices .....	4
Read-Write Devices .....	5
Specialty Applications .....	8
Documentation .....	8
Forensic Tools .....	9
UltraKit .....	9
EnCase .....	9
FTK (Forensic Toolkit) .....	9
ProDiscover .....	10
Paraben .....	10
WinHex .....	10
DiskEdit .....	10
Norton Ghost .....	10
Transend Migrator .....	11
IsoBuster .....	11
Stego Suite .....	11
NetAnalysis .....	11
Other Forensic Tools .....	12
The Role of Computer Forensics in Internal Control .....	12
Computer Forensics .....	12
Internal Control .....	13
Preventive Controls .....	15
Detective Controls .....	16
Corrective Controls .....	17
Incorporating Computer Forensics in a Self Governance Program .....	17
Structure and Management .....	18
Resources .....	20
Methods .....	21
Conclusion .....	22

## Securing Your Electronic Information Under Sarbanes-Oxley

by

Gregory L. Fordham, CPA, CIA, CCE

On July 30, 2002 President George W. Bush signed into law the Sarbanes-Oxley Act (P.L. 107-204, 116 Stat. 745). The Sarbanes-Oxley Act was developed in response to the Enron, Worldcom and more than twenty other corporate debacles related to financial reporting irregularities. Although the Act was initiated in response to the Enron demise in late 2001, the Worldcom collapse in mid 2002 is credited with inspiring enough lawmakers in Washington to ensure its passage.

According to President Bush, the Act was designed to protect investors by improving the accuracy and reliability of corporate disclosures that are made pursuant to securities laws, and other purposes. Although most of its provisions are directed toward financial statement reporting of publically traded companies, the Act also incorporates several provisions that are intended to prevent fraud. These provisions include whistleblower protections and self governance programs. Specifically, Section 806 of the Act amends ¶1514A to protect whistleblowers in fraud cases. Also, Section 301 of the Act charges the audit committee with the responsibility to establish procedures for receipt, retention and treatment of complaints by the issuer regarding internal controls, accounting or auditing matters, and confidential whistleblower submissions.

In addition to implementing fraud prevention measures, the Act facilitates discovery and investigation of improper activities by imposing various penalties for the destruction, alteration or falsification of records. For example, Section 802 of the Act amends ¶1519 of Chapter 73 of Title 18 USC and imposes penalties for destruction, alteration, or falsification of records in Federal investigations and bankruptcy. Similarly, Section 1102 of the Act amends ¶1512 of Title 18 USC and imposes penalties for document destruction to impair objects integrity in official proceeding. Both of the provisions have far reaching implications that extend beyond a whistleblower investigation. Indeed, they extend to the everyday activities of covered organizations as they decide how to manage their data repositories as well as place increased obligations on organizations for preserving their data once a whistleblower charge has been received.

This article does not consider routine data retention policies. Rather, the focus of this writing is the preservation of data in response to whistleblower complaints under the Act and the use of computer forensic as an internal control technique and part of a self governance program. The first topic, electronic information when responding to whistleblower actions, examines the various sources of

electronic data as well as the need for data preservation and the special analysis tools required for electronic data analysis. The second topic, the role of computer forensics in internal control, examines the nature of internal control and computer forensics in order to explain how computer forensics can be used to prevent, detect and identify weaknesses and breaches in internal control. The final topic, incorporating a computer forensics program in a self governance program, examines the requirements of the Act and how computer forensics can be used both proactively and reactively as part of that program.

## **Electronic Information When Responding to Whistleblowers**

Electronic information is increasingly critical when investigating whistleblower claims. The importance of electronic data is increasing for two reasons. First, it is critical because so much about business is being conducted electronically. Second, it is critical because electronic data is more fragile than its traditional paper based counterpart. Simply by continuing to operate a computer valuable evidence relevant to the whistleblower claim could be destroyed or altered. Both of these factors are important considering the provisions of the Act that impose penalties for destroying or altering documents.

### **Data Sources**

In order to avoid triggering the penalties imposed by Sections 802 or 1102 of the Act, covered organizations need to immediately start preserving their electronic data whenever an official investigation is initiated by any department, agency or bankruptcy proceeding. These same procedures should be implemented whenever a whistleblower complaint is received so that it can be properly evaluated.

The first step in preserving electronic data is to identify the various data sources. The data sources are typically many as are the methods for handling them. Just some of the items that should be considered are those immediately accessible to the individuals involved such as personal computers and related accessories. Next, other data storage locations that should be considered are those located on shared devices and network resources. Finally, the data held in specialty devices and applications like e-mail servers, content and records management systems, and applications databases should be preserved. Each of these data sources and the methods for preserving their data are discussed in the following sections.

### **Personal Computers and Accessories**

Personal computers includes the individual computer workstation and/or laptop computers. The data to be preserved on these devices includes both their internal storage devices, which are usually hard drives. Other technologies exist, however, such that the internal storage of a workstation or laptop computer could also include flash cards.

The accessories to a computer include a variety of different media such as compact disks (CD) and digital versatile disks (also known as digital video disks or DVD for short). Although used less frequently these days, another type of external storage device is a diskette and ZIP disks which are a kind of super diskette. Newer to the technology spectrum are memory sticks, also known as thumb drives, flash drives and/or jump drives. These tiny devices, that are about the size of a disposable cigarette lighter, plug directly into a computer and commonly have as much capacity as a CD but can be found with capacity equaling a DVD. Also becoming very common are external hard drives that connect to a computer in the same manner as a memory stick, by way of Universal Serial Bus (USB) or firewire.

As technology evolves the lines are blurring between personal computers and other devices. Some examples of this group include personal digital assistants (PDAs) and cell phones. These days such devices provide both their historical features as well as many others all bundled into one device. Still another example is the iPod that can connect to a computer and be used to store data files.

### **Shared Devices**

After considering all of the personal devices one must start to broaden the net to consider many data sources that are not so personal such as the network. After all, some would say that the network is the computer.

Virtually no computer stands on its own any more. Rather they are all interconnected to not only facilitate cooperative efforts but to share resources like printers, storage areas and other specialized services. Data sources for network data should include both on-line and off-line storage media.

On-line storage media are the readily accessible storage like the user directories and departmental shares on a file server or network attached appliance. The off-line storage media will include archival and disaster recovery systems and their media such as tapes.

### **Specialty Devices and Application Databases**

The next category of data source is the more specialized computer systems such as e-mail, content managers and document managers and application databases. Everyone is familiar with the e-mail server. It acts like the local post office for all the users connecting to that server. Users use their server mailbox to send and receive mail and often to store mail. Thus, with the prevalence of e-mail this data source becomes an important source of electronic data and one that is always high on the preservation list.

Enterprise content managers and record managers are designed to satisfy the organization's record retention requirements. They are typically useful in large organizations where uniform applicability of an organization's record retention policies across hundred or thousands of employees can be difficult. Thus, these systems enable a central administrator to push down to individual employee machines the rules that should be followed for retaining an organization's electronic data. The rules

can include what to retain and what to discard, as well as where the retained documents are to be stored and organized.

Finally, there are application databases. These systems are found in almost every business application from financial accounting to human resources to project management and intellectual property. They essentially retain records related to individual transactions and provide management with an automated means for managing and reporting on this data. Historically, people have focused on the paper based reports that are generated by these systems. In recent times, however, they have learned that there is often far more data available in an application database than ever is presented on paper and that often times this data includes audit trail and identification features that are essential to an investigation.

## **Preservation Methods**

Preservation is often quite simple and not as expensive or time consuming as many might believe. The important part is to get the data preserved and then the more expensive and time consuming part, the analysis, can be performed in accordance with an appropriate plan.

This is a good place to remember that the preservation phase is not the place to cut corners. Preservation is typically not that expansive or expensive. So, there is really not a lot to be gained by cutting corners during the preservation phase. Also, everything that comes later depends on how well the preservation phase was performed. Once it has passed, the data can never get any better.

During the preservation phase every case should be treated as if it will end up in court. It is easier to regard the computer as evidence from the start and ease up on the subsequent evidentiary analysis phase if it is determined that there is no substance to the issue. The opposite approach, however, is not impossible. So, it is best not to start working with the computer data in a casual manner and then realize that there is a problem. By that time it is often too late to start treating the data as if it were evidence. Instead, treat it as evidence from the start and practice good preservation methods. The particular techniques that should be employed will depend on whether the data to be preserved is located on a read-only device, a read-write device or specialty applications.

## **Read Only Devices**

The easiest place to start a preservation effort is with the read-only devices such as CDs, DVDs, and tapes. These items are the easiest because they can be preserved simply by taking physical custody of them and storing them in a secure location. If they should happen to contain data that is needed, then it is fairly easy to make copies of their contents and provide a working copy back to those that need the data.

When making copies of these devices it is also good to remember that CDs and DVDs can contain multiple sessions. These sessions will not be visible when the contents of the CD or DVD are viewed through the Windows Explorer. It takes other types of CD viewers.

Evil doers wanting to hide their activities can use this fact to create new sessions on top of the data that they really want to hide. Consequently, to be sure and copy all the data on a CD one must perform a track-to-track copy. If, instead, the copy is accomplished using drag and drop features of Windows only the last session will be copied to the new CD or DVD.

### **Read-Write Devices**

Things become more complicated when preservation moves to the read-write devices such as personal computers, PDAs, cell phones and memory sticks. After all, simply operating a computer or examining these devices without taking special precautions to protect their contents can alter their data. Typically the dilemma is that these devices are likely needed for continuing business operations. So, it is unlikely that preservation can be accomplished simply by taking custody of them and storing them in a secure location. Thus, these devices will likely need to be copied.

The exact copy method that should be used can be guided by several factors. If the device is a personal computer there are several options. If the device is immediately needed for service then the simplest method is to perform a drive swap.

A drive swap can be performed by using special software, like Norton Ghost, to copy only the active data, including system files, from the original drive to the replacement drive. By only copying the active data, the copy process will be faster than if the entire drive, including free space, is imaged. Furthermore, there is no need to copy the free space containing deleted data. By deleting the data the user has already determined that the information is not needed for continuing operations. After completing the copy process, the original drive is taken into custody while the replacement drive is installed in the target machine and business operations continued.

Drive swapping is always an option that should be considered. The only issue is should the swap be performed after a forensic grade image is created and should the replacement drive be created from the forensic grade image. Some professionals may want to take more cautious approach and not want to risk anything happening until after the forensic grade image is created. For example, if the Ghosting process is accidentally performed in reverse then the original drive will have copied to it all the active data, if any, from the replacement drive. Also, some may not want to risk having the computer accidentally boot into an unprotected state where the metadata of files on the original drive could be altered.

Certainly, all of these risks are possible but there are methods for protecting the original drive from the effects of Murphy's law. First, disconnect the original hard drive from its connection while configuring its host system to boot from a floppy drive or CD drive. Next, perform the Ghosting with the original drive in the drive 0 (zero) position. Ghost will not allow images to be copied back onto the zero position. Finally, use the Ghost DOS based executable on a properly prepared DOS boot diskette or CD. In order for the DOS diskette to be properly configured remove any references to the original hard drive from the system and configuration files on the boot disk.

Drive swapping is not always practical. A court order may not contemplate drive swapping. Similarly, in enterprise situations it may be impractical from a timeliness perspective or from a notification perspective to perform a drive swap. Since a forensic grade image is considered the evidentiary equivalent of the original, there technically is no real need to retain the original. Rather, retention of the original is desirable only if questions later arise about the validity of the imaged copy.

In those cases when drive swapping is not practical, a forensic grade image is the next best option. A forensic grade image is a bit stream, sector by sector copy of the original. The image can either be copied to a file or replicated/restored to another hard drive device. The latter process is often referred to as a clone, since it is a working copy of the drive. This is different than the former in that when the image is copied to a file, the image cannot be used to boot the computer. Nor is it otherwise functional. This state is frequently preferred over the clone version because of the file's increased resistance to alteration and increased protection of the imaged data that is encapsulated in the file format.

As with the working copy process described previously, special procedures will be required when making the forensic grade image to ensure that no changes are made to the original prior to completion of the imaging process. The image must be made in an environment that will not alter evidence on the original drive or it must be performed with the assistance of write blockers that protect the original drive from alteration.

Creating forensic grade images can take more time than drive swapping. The increased amount of time is caused by the technical difference in the process as well as by the additional assurance steps that are now practiced. As explained previously, the drive swap will copy only the active data while the forensic grade image will identically copy all data on the hard drive, including the free space on the drive. Additional time will also be required for verification of the forensic image. Even when tested and reliable imaging tools have been selected for making the image, current best practices require that the image be verified by at least one of two options. The first is by re-imaging with different equipment and then comparing the MD5 hash, or equivalent, of the first image to the MD5 hash of the second. In the alternative, one could also compare the MD5 hash or equivalent of the original drive to the MD5 hash of the image. Either method will require making at least two passes over the original drive.

An MD5 hash is a one way algorithm that computes a unique value for a data stream like the contents of a file or the contents of an entire hard drive. The MD5 hash is but one of many such algorithms. The MD5 hash was developed in 1994 for use in electronic signature authentication. It has been widely used in computer forensic applications as a means to determine whether two data streams are unique or identical

In recent times the MD5 hash has come under attack, since it has been determined that collisions are possible, particularly when the two data streams are very short such as a date. A collision is where two different data streams produce identical MD5 results. As the data streams increase in length and complexity, however, it is believed that the chance of collisions diminishes.

Interestingly, the MD5 hash was never incapable of experiencing collisions. Rather it was just believed that with the chances at less than 1 in 2 raised to the 128<sup>th</sup> power that collisions were very unlikely. (2 raised to the 128<sup>th</sup> power is about the same as 3.4 times 10 to the 38<sup>th</sup> power or the number 34 followed by 37 zeros. Thus, the results produced by a MD5 hash are statistically far better than those experienced in DNA analysis.)

In any event, performing the verification can take considerable time and this would be in addition to the time required to perform the original image. Naturally, if the verification process does not produce identical results then another imaging or verification attempt will be necessary. Thus, it is easy to see how the imaging process can take far longer than simply performing a drive swap and retaining the original. Of course, at some time the imaging will have to be performed but if the goal initial goal is to reduce the cost of preservation and to reduce disruption to the organization then performing a drive swap in the field is a more efficient alternative than performing a drive imaging in the field.

Other than computer hard drives there are several other types of read-write devices that will need special processing in order to properly preserve their data. Memory sticks, cell phones, digital camera, PDAs, digital voice recorders, and all other kinds of digital recorders will also need special processing. The precise manner in which the data on those devices can be preserved will depend on the type of device and the manner in which one can connect to the device.

Memory sticks can usually be imaged similar to a hard drive but a special write blocking device matching the memory stick's connection is needed. Digital cameras and the removable memory chip in cell phones are similar to memory sticks but also require a special device for reading their flash memory chip in a protected mode.

PDAs, voice recorders and the embedded storage devices of cell phones can be more troublesome because they typically require special imaging tools. In other words, the same tools for imaging hard drives and the other devices previously discussed cannot be used on PDAs, voice recorders or the embedded storage of cell phones.

After all of the read-write personal devices have been preserved, the next storage category is the shared storage devices like network servers and other storage devices. Network storage devices introduce another set of issues. One of the evolving problems is the sheer size of network storage devices. In recent times the storage capacity of these devices has become very large. As a result, imaging can take many hours and even several days to complete. Thus, performing the image while minimizing business interruption can require careful scheduling.

Another complexity introduced by network storage is the configuration of storage media. Often the media is assembled in a RAIDed configuration. RAID stands for Redundant Array of Inexpensive Disks. In other words the large capacity of the network device is not accomplished with a single large capacity hard drive but by taking many hard drives and configuring them so that they operate as if they were a single device. This configuration can mean that individual drive imaging is not practical. As a result, a different approach is required and usually results in imaging the entire array as a logical device instead of a lot of physical devices.

Other than the technical challenges, the particulars of network storage also introduce some practical challenges as well. In other words, if the total data storage volume is large but the area of interest is small, such as a single directory or folder, the question arises whether imaging the entire storage device is even warranted if the information of interest can be obtained from other data sources such as backup tapes. Since the server is not being used by an individual some of the things that one would expect to find in the free space of the drive on a personal computer (such as application temporary files that are created when one views a document or link files pointing to the location of the document or internet history files) will not be found on the shared network device. So, if a good backup tape history exists one might not expect to find much more on the network device than what would exist already on backup tapes. If not, one might choose to simply take the key artifacts such as files as they currently exist, access logs and other user related information.

### **Specialty Applications**

E-mail and other specialty applications such as databases are the next area of preservation interest. For these items, it might not make sense to preserve the entire device on which these applications reside, if all that is of interest is a smaller set of data within the application itself. E-mail is a good example of this condition. What is the practicality of preserving an entire storage device if all that is of interest is a few mailboxes within the e-mail data store? This is particularly true when the e-mail system encapsulates all of its data within a database file. In such a case there will not be a lot of remnants of deleted e-mail scattered around the storage device, particularly when the device is only a storage location and is not the viewing location of the e-mail data. Thus, in these cases it may be just as suitable to preserve the e-mail data store along with the individual mailboxes of the persons of interest. There would be little else to gain, if anything.

Content managers and records managers provide another specialty application. These programs help an organization to retain and manage its record retention policies. They may or may not actually store the data. Rather, they may only point to the location and organization of the data that is stored elsewhere. If they do, in fact, store the data then one would want to determine what data is available and the best way that it should be extracted from these system and preserved.

Application databases also provide a special set of issues. Most notably is that there may not be any real need to image the storage devices on which they reside, which could be quite large, if an adequate history can be obtained by preserving historical backup tapes. At most the entire database file will need to be preserved but at a minimum there may be ways to select only the desired data from all of the data that is contained within such a system.

### **Documentation**

In addition to performing the preservation it is also important to begin documenting the chain of custody of the preserved data. This should be begin by inventorying the items and recording the date on which they are taken into custody along with any unique identifying marks such as serial numbers, etc. When the items are taken into custody it may not be a bad idea to take photographs

of the data, particularly if they involve the contents of a person's office. In that case it is good practice to take pictures of the office and record as part of the preservation effort exactly where the item was found. This extra step will be helpful later on when the dispute is exactly what was found, where it was found and why something else was not found that someone claims should have been there.

## Forensic Tools

Like any other forensic science, computer forensics involves the use of sophisticated technology, tools and procedures which must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing. Typically, computer forensic tools exist in the form of computer software but there are also specialty hardware devices such as write blockers and other interface devices used for reading the analyzed media.

Computer forensic specialists guarantee the accuracy of evidence processing results through the use of established evidence processing procedures and through the use of multiple software tools, developed by separate and independent developers. In more recent times, there is an increasing number of vendors providing forensic tools. This provides analysts with more tools to choose from and more features available in those tools.

There are a number of tools and different types of tools that are required. These tools include write protection devices, imaging and preservation tools, and analysis tools. Some of the most widely used tools are discussed in the following sections.

**UltraKit by Digital Intelligence in Waukesha Wisconsin.** The UltraKit is a collection of various hardware write blocking devices. Hardware write blockers are devices that sit between the hard drive and the computer. These devices stop signals from being written to the hard drive while fooling the computer and its operating system that the signals are being written. The collection includes Firewire, USB, IDE, serial ATA, and SCSI interfaces.

**EnCase by Guidance Software in Pasadena California.** EnCase is one of the most widely used computer forensic tools around the world. It contains both an imaging engine and analysis environment. The analysis environment provides the ability to examine the file system and remnants of the file system, recover deleted files and file fragments, examine the data on the media directly at a low level, search the contents of the media for key words, perform hash and signature analysis and develop scripts to automate the examiner's analysis. EnCase is available in single workstation and enterprise versions. The enterprise version allows examiners to perform their examination remotely. While the remote examination feature is attractive, it also comes with a six figure price tag that makes many organizations look for alternatives.

**FTK (Forensic Toolkit) by Access Data in Lindon Utah.** FTK is also one of the most widely used computer forensic tools around the world. Like Encase it contains both an imaging engine and an analysis environment. The FTK analysis environment provides many of the same abilities as the EnCase environment. It does not contain a scripting language however. It is also more limited than

EnCase in the number of file systems that it can interpret. For example, it cannot interpret the file system used on Apple computers. FTK is available only for workstation analysis. Thus, it is not available in an enterprise version like EnCase that allows imaging and analysis from remote locations. To a certain extent, FTK's focus on its areas means that it often provides features in those areas that are not available or implemented as well in other tools like Encase. For example, FTK is considered to have stronger e-mail and internet analysis tools than EnCase and FTK provides built in password cracking, while EnCase users must rely on third party tools.

**ProDiscover by Technology Pathways in Coronado, California.** ProDiscover is another widely used computer forensic tool that contains both an imaging engine and an analysis environment. Since it is a relative newcomer to the computer forensic field it has not yet developed the vast following of EnCase or FTK, although it contains many of the same features and capabilities. It even contains an enterprise capability that allows imaging and analysis from remote locations across any TCP/IP network. Although ProDiscover provides many of the same features as EnCase and FTK, as the new kid on the block it offers some price advantages, particularly with its enterprise capability which is priced at about one-tenth of EnCase.

**Paraben by Paraben Corp. in Orem Utah.** Paraben is another widely used computer forensic tool that contains both an imaging engine and an analysis environment. Paraben entered the computer forensic market with a specialty in handheld devices such as PDA's and cell phones. It has since expanded its product offering to include the traditional imaging engine and analysis environment for hard drives and other computer media.

**WinHex by X-ways Software Technology, AG in Cologne Germany.** WinHex is a Microsoft Windows based hex editor. A hex editor is a low level analysis tool, which means it permits analysis of data below the file level. Thus, it allows users to view data as it exists directly on the computer media at the byte and sector level. WinHex is just one in a family of computer forensic tools provided by X-ways Software that provide media imaging and analysis capabilities. Although very powerful, WinHex is not as user friendly as the integrated packages like EnCase, FTK and ProDiscover. Nonetheless, it offers some capabilities and features that are not as robust or fully developed by these other packages.

**DiskEdit by Symantec in Cupertino California.** DiskEdit is a Microsoft DOS based hex editor. It dates back to the early days of computer forensics when examinations were performed using clones under a DOS environment. Since under DOS there was little concern about the operating system altering the computer data, write blockers were not needed. In fact, about all that was needed was to disable certain programs, by not calling them on machine boot-up. Although less useful than in times past, low level editing tools like DiskEdit and WinHex should still be included in any forensic toolkit.

**Norton Ghost by Symantec in Cupertino California.** Norton Ghost is a Microsoft Windows and DOS based imaging engine. It is widely used by IT professionals for replicating base images to computer workstations in the organization. In other words, an organization may have a basic configuration for the computer workstations used by employees within the organization. This configuration is preserved as an image that can be repeatedly restored to workstation hard drives.

In addition to this capability Ghost can also copy the working configuration of one drive to another (active data only) as well as produce forensic grade image of a drive where all sectors are copied to a raw image file. These latter capabilities can be useful for preserving electronic evidence either as a forensic grade image or through a drive swap. A drive swap is where the active data of the original drive is copied to the a new hard drive that is then swapped with the original. The original drive is retained as evidence while the new drive allows the user to continue with normal business operations with little disruption in business activities. The raw data image file is similar to what is performed by other forensic tools with imaging engines like EnCase and FTK.

**Transend Migrator by Transend Corp. in Palo Alto California.** The Transend Migrator is an e-mail migration tool. In other words it allows users to migrate e-mails contained in one kind of data store like Lotus Notes to another kind of data store like Microsoft Exchange or Microsoft Outlook. The most likely use of this kind of tool involves the recovery of e-mail stores from backup tapes or extraction of particular mailboxes from an e-mail data store. Without such a tool the recovery of e-mail that has been preserved on backup tapes or other archival media requires rebuilding the e-mail server in the condition that it existed at the time that the backup was made. This can often be time consuming and filled with trial and error as the exact combination of software versions and patches are configured.

**IsoBuster by Smart Projects, Smart-Projects.net.** IsoBuster is a tool for examining CDs and DVDs. Although this feature is provided in many of the integrated packages like EnCase and FTK, the full range of various CD and DVD formats is not always supported by those products; hence, the need for a specialty product like IsoBuster. The examination of CDs and DVDs is not as straight forward as one would expect. It is a frequent practice of the evil doers to disguise their activity by overwriting their last activity with another burning session. Then, when the CD or DVD is placed in a CD or DVD reader for review all that will be seen by a user is the last session, even though earlier sessions exist with hidden data. To see and examine these earlier sessions, one would need an analysis tool like IsoBuster.

**Stego Suite by WetStone Technologies, Inc. in Cortland, New York.** The Stego Suite is a bundle of several software tools designed for the detection, analysis, and recovery of digital steganography. *Steganography* (literally meaning “covered writing”) is the process of hiding information within other information. Steganography and its close cousin digital watermarking were originally developed to enable the rightful proprietor of electronic data to hide signature information within digital data files (thus enabling the rightful owner to prove his ownership of the digital data at some future time). Unfortunately, this same technology can also be used to hide customer lists, business plans, and computer source codes in files as innocuous-looking as vacation or family photos that are e-mailed from work to home by an employee before his departure from the workplace (or even from a current employee to a departed employee). Because such hidden data within a photo file is imperceptible to the eye, as is the alteration made to the photo, a reviewer of the data cannot detect its existence without special software like Stego Suite and/or access to the unaltered original file.

**NetAnalysis by Digital Detective in United Kingdom.** NetAnalysis is a tool for examining internet history and cache pages.

**Other Forensic Tools** - The above referenced tools are by no means an exhaustive list. Indeed, the increasing interest in computer forensics and information security has translated into an ever increasing pool of vendors and technologies. Since the list is always changing, readers are encouraged to search the web for terms like computer forensics as well as other discriminating terms that appear in this writing.

## **The Role of Computer Forensics in Internal Control**

Section 302 of the Act establishes that signing officers are responsible for establishing and maintaining internal control. In addition, they are to evaluate the effectiveness of internal control and report on their conclusions. Although the Act is primarily focused on financial statement reporting, it is also interested in the adequacy of the internal controls necessary to assure the accuracy of those reports.

In the modern business environment, where so much activity is performed with the use of computerized equipment, computer forensics should be an integral part of an organization's internal control structure. The following sections further discuss the nature of computer forensics and its use as an element of internal control.

### **Computer Forensics**

Computer forensics has become a popular topic and is increasingly widespread. Its popularity has increased as a result of the widespread use of computer equipment. After all, there would be no need for computer forensics if there were no computers.

While some may refer to computer forensics as the autopsy of a computer hard drive it is actually much more than that. In fact, it is probably better defined as the application of various science and engineering disciplines to the collection, analysis and interpretation of digital evidence. Or stated another way, computer forensics is the scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the information can be used as evidence in a court of law.

Interestingly, there is a link between computer forensics and an organization's financial position. In a nation of laws, citizens protect themselves by asserting or defending claims in court. In order for computer evidence to be accepted in court, it must be properly collected, verified and handled under accepted computer forensic procedures. If an organization cannot collect computer evidence in a manner that preserves its admissibility in court, it may not be able to prevail in the assertion or defense of its legal claims. If the organization is unable to prevail in its legal position then its financial position may be compromised as well.

The benefits of computer forensics are not limited to the ability to present evidence in court. After all, computer forensics is as much an analysis and investigative science as it is a collection and

presentation science. Thus, there are two added benefits. The first is the visibility that computer forensic tools provide into operational areas of a computer. With this visibility investigators can more accurately confirm the proper or improper workings of computer software.

The second benefit is also related to the investigative power of computer forensic tools but is actually more of a control mechanism. Stated more precisely, because of the increased investigative power of computer forensic tools, evil doers have a greater chance of having their activities and themselves discovered. As a result, computer forensics is a deterrent to those wishing to be mischievous.

As a result, computer forensics is an essential element of internal control for three reasons. First, it is a better way for an organization to evaluate the success and effectiveness of its computer based internal controls. Second, its investigative capabilities provide a strong deterrent, which alone is a type of preventive control. Finally, its acceptability in court can bolster an organization's financial position.

## **Internal Control**

Control, in general, is accomplished by setting standards, measuring against those standards for success and making corrections if needed. Internal controls are the controls implemented within an object that is to be controlled. With regard to an organization, internal control is all the means used to promote, govern and check upon various activities for the purpose of seeing that the enterprise's objectives are met. Thus, internal control of an organization can include or exclude whatever management chooses to control or not to control.

Although Section 302 of the Act imposes certain requirements regarding internal control, it does not provide any specific guidance about what internal controls are required. Rather, it requires only that internal control be adequate to ensure that material information is made known to the signers of the financial reports and that the signers produce reports and other disclosures about the effectiveness of their internal controls.

Under the Act, therefore, the objectives of internal control are rather narrow. Indeed, they are focused on the material accuracy of financial reporting, since the Act requires only that, "[T]he signing officers . . . have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities."

The limits of the Act's requirements are more obvious when contrasted with the objectives of internal control as described in the professional standards of internal auditors. Internal auditors are professionals who specialize in the evaluation of internal control. They have broadly described the breadth of internal control in their 300 series of professional standards. In fact, Professional Standard 300.05 identifies the five primary objectives of internal control as:

- Safeguarding assets;

- Compliance with policies, plans, procedures, laws and regulations;
- Accomplishment of objectives and goals for operations and programs;
- Reliability and integrity of information; and
- Economical and efficient use of resources.

When the above objectives are compared to those required by the Act, it is easy to recognize that the Act considers only the reliability and integrity of information. Even safeguarding of assets, a traditional part of accounting internal control, is arguably absent from the Act's requirements if the loss of those assets has been detected by the organization's internal controls and accurately reported in the financial statements.

External auditors, who are those attesting to the representations contained in the financial statements, have long recognized that an organization's internal control structure contains policies and procedures that are not relevant to an audit of the organization's financial statements. Those that are relevant have historically been limited to the ability to record, process, summarize, and report financial data consistent with the assertions embodied in the financial statements.

In response to the Act, the Security and Exchange Commission (SEC) issued its own definition of internal control in its Release No. 33-8238. In that release, the SEC defined internal control as:

*A process designed by or under supervision of the registrant's principal executive and principal financial officers, or persons performing similar functions, and effected by the registrant's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that*

- *Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transaction and dispositions of the assets of the registrant;*
- *Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and receipts and expenditures of the registrant are being made only in accordance with authorization of management and directors of the registrant; and*
- *Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the registrant's assets that could have a material effect on financial statements.*

Clearly, the SEC has defined internal control, for purposes of the Act, in a manner that is relatively similar to accounting internal control. According to the SEC, internal control includes those policies and procedures to ensure reporting accuracy and safeguarding of assets; however, the definition also includes policies and procedures that assure prevention and timely detection of improper use or disposition of assets that could have a material effect on the financial statements.

There are basically three types of internal control. They are preventive, detective and corrective. All three stages of control (preventive, detective and corrective) are mentioned in Section 302 of the Act. As stated in the final bullet point above, internal controls should provide reasonable assurance that unauthorized acquisition or disposition of assets are prevented or timely detected. Also, the report on internal control required by Section 302 should indicate any corrective actions taken as a result of deficiencies and material weaknesses discovered.

Since so much of an organization's activities involve, and even depend on computerized systems, the use of computer forensics is a logical addition to an organization's internal controls. An effective use of computer forensics in evaluating internal control should not be limited to performing a post mortem after internal control was breached. Rather, they should be implemented in each of the three stages of control; preventive, detective and corrective. The manner in which computer forensics can be used in each of the three stages of control are discussed in the sections that follow.

### **Preventive Controls**

Preventive controls are those that are built into a system to prevent an error, or undetected event, from happening. The text book example of a preventive control is a locked door. Another is segregation of duties; custody of assets, recording of transactions, and approval of transactions. With respect to electronic data, preventive controls are usually divided into physical, logical and application controls

Physical controls involve access and usage restrictions to computer hardware, system and application software and the electronic data itself. These types of controls would include those that are part of physical security such as personnel badging and restricted access areas. Some of the more sophisticated physical controls involve preventing the use of certain devices such as thumb drives, which are a common means of trade secret theft and introduction of malicious software.

Logical controls are those things like user authentication, security policy management and other access features offered by the computer system itself. Logical controls are not limited to those provided by the computer system's manufacturer. They can also include third party solutions designed to secure computerized data with additional layers of encryption and other access control techniques.

Application controls include various user access and data validity checks commonly found in system and application software. User denial of application features as well as drop down boxes with pick lists are common examples of application controls.

There are two different ways in which computer forensics can function as a preventive control. The first involves support during audits of logical and application controls. In this effort, computer forensic tools can be used to monitor testing and review system artifacts during the audit of logical and application controls. A review of these artifacts and systems monitors would confirm that logical and applications controls are working properly and have not been compromised.

The second way in which computer forensics can serve as a preventive control is as an investigative tool. As stated previously, computer forensics as an investigative tool is a preventive control because it is a deterrent. The increased investigative capability of computer forensics and its ability to collect and present evidence that is acceptable in court increases the chance that the malevolent employees or other individuals will be caught and suffer consequences for their actions. The increased deterrent effect resulting from a higher probability of detection is a preventive control. The preventive control element of computer forensics, however, is directly related to its ability as a detective control as discussed in the following section.

### **Detective Controls**

Detective controls are designed to alert management of errors or problems as they occur or shortly thereafter. An alarm that sounds when a locked door opens is an example of a detective control. Whistleblower hotlines, e-mails and other anonymous reporting mechanisms are also examples of detective controls that are designed to identify unwanted activity.

With respect to electronic data, detective controls begin with the physical and logical controls discussed above. All access controls could log their results, pass or fail, into access control logs for subsequent review and analysis. In addition, thresholds could be set that after failing an access control attempt so many times that a special alarm is sounded requiring immediate attention.

Computer forensics, as a detective control, goes beyond the traditional system imposed controls. Computer forensic analysis could be used in response to whistleblower complaints to collect and analyze electronic evidence or employed on a real time basis to review and evaluate system integrity and the effectiveness of other computer based internal controls.

The use of computer forensics in response to Whistleblower complaints was discussed in the first section of this writing. With respect to real time detective controls, computer forensic techniques can be used to search and analyze all computers connected to a network for violations of company policies and/or the existence of malicious software (malware) used to breach other physical, logical and application controls. For example, enterprise tools such as EnCase and ProDiscover could be used to perform signature analysis and hash analysis to find unauthorized software and data files as well as detect attempts to hide these efforts.

*Signature analysis* is a comparison of file extensions to known *byte patterns* within the file itself. This enables the examiner to detect changes to a file extension which the user may have been made to hide the importance of a file.

*Hash analysis* utilizes a known value determined by a message digest algorithm (an example is the MD5 message digest) to detect prohibited conduct such as the installation of prohibited software. Similarly, after a breach has been discovered or a complaint lodged, this method could be used to find other instances of the software or data.

Also, computer forensic techniques can be used to confirm the traditional segregation of duties and that other internal controls have not been compromised. Reviews of access control logs could be performed to verify that those responsible for approving transactions are not also using application software to record transactions.

While computer forensics may be an effective detective control, its ability to correctly identify malevolent individuals is limited if access and security controls are poorly implemented. Thus, the importance of basic security controls cannot be overstated because without these the effectiveness of computer forensics as well as the other controls is weakened.

There are still other basic steps that can be taken to enhance the effectiveness of computer forensics as a detective control. Since evil doers will always try to cover their improper activities, the ability of the computer forensic technician to detect their activity either proactively or reactively can be enhanced if the data to be analyzed is not limited to what remains after the event. In other words, the consequences of improper activity as well as the methods by which the result was achieved can be easier to detect and more fully understood if frequent historical snapshots with full system state information are available for analysis. Thus, organizations should ensure adequate backup and data retention horizons that include both active data as well as low level and system state information.

### **Corrective Controls**

Once events have been identified through preventive or detective controls, the third type of internal control is a corrective control. Corrective controls are used in conjunction with detective controls to recover from the consequence of the undesired events. The text book example of a corrective control is a guard to apprehend the intruder who forced open the locked door and sounded the alarm.

With respect to electronic data, corrective controls can again include physical, logical and application security controls. For example, after user authentication has failed a predetermined number of times, that user's access rights could be suspended pending investigation of the failed attempts.

With respect to computer forensics corrective controls could include seizure of a computer hard drive or other electronic evidence after determining that it contained improper materials. Similarly, seizure could be part of the corrective control in response to a whistleblower complaint. Even if seizure is not advised, many of the enterprise computer forensic tools contain features that permit monitoring and analysis of individual computers remotely and in a stealthy fashion.

## **Incorporating Computer Forensics in a Self Governance Program**

Title III of the Act is named Corporate Responsibility. It includes eight sections, 301 through 308, that address various attributes of corporate self governance. While the Act does not specify the exact procedures or methods that organizations should employ when designing and implementing their self governance programs it does provide broad performance standards.

As described previously, Section 302 designates the signers of the organization's quarterly and annual reports as the person's responsible for the accuracy of those reports and for designing, maintaining and evaluating the effectiveness of the internal controls necessary to ensure the accuracy of those reports. In addition, Section 301 of the Act requires covered organizations to establish audit committees. The audit committee is required to establish procedures for receiving, retaining and responding to:

- Complaints relating to accounting, internal controls and auditing; and
- Information submitted by anonymous employees relating to questionable accounting or auditing matters.

Thus, the audit committee is responsible for overseeing whistleblower complaints for matters governed by the Act whether or not they originate from anonymous sources. The separation of duties between approving reports and responding to whistleblowers is a significant enhancement to the organization's internal control structure imposed by the Act.

Since the preceding sections of this article have examined the use of computer forensics in responding to whistleblower complaints under Section 301 and as part of the internal control structure under Section 302, the following section examines the manner in which the computer forensic effort should be incorporated within the overall self governance program. More specifically, the following sections examine the structure and management of the computer forensics effort, the resources required and the methods that would be employed.

## **Structure and Management**

A self governance program is part of an organization's internal control structure. This structure is not only multifaceted, as evidenced by the various objectives of internal control and differing types of internal control, it is also multi-layered. In fact, it now requires at least three layers.

The first layer of the control structure is provided by management. Management is primarily responsible for internal control. They, typically, determine the need for controls, design the controls, implement the controls, and then evaluate the controls that they have designed and implemented.

Management's effectiveness, however, in controlling the organization and accomplishing its objectives are the responsibility of the Board and other senior executive officers. They cannot rely entirely, nor should they rely entirely, on management's representations. Rather, they require an independent body on whose opinions they can also consider. Historically, the internal audit department has provided the independent assessment of management's performance to the Board and other senior executive officers.

Under the Act, the Audit committee now also takes a more prominent role in the organization's internal control structure as the entity responsible for whistleblower complaints. Historically, this

function was delegated to management and likely contributed to ignored warnings that might have prevented Enron and Worldcom type disasters. Thus, the Audit committee comprises the third layer.

With regard to computer systems and the use of computer forensics, management will likely use the Information Technology (IT) department as their tool for monitoring and assessing internal control. After all, many facets of an organization's computer security are logically embedded as a line function within the IT department. Since the IT department is part of management, however, it is not well suited for providing an independent appraisal of internal control. Its lack of independence also compromises its ability to assist the Audit committee in investigating whistleblower complaints.

The internal audit department has long served the Board and other senior executives with an independent appraisal of computerized system operations and internal controls. Computer auditing, internal controls governing computer systems, computer security and even computer forensics are disciplines held by internal auditors. In addition, the internal audit department is usually organized so that it not only has independence but has the clout necessary to cross organizational boundaries and accomplish its investigation without compromise. Also, internal auditors are accustomed to the investigative, documentation and reporting processes that accompany a self governance program. In addition, such skills are part of their training and professional standards.

While continuing evaluation of internal control could be satisfied by the internal audit department, a whistleblower action is another situation entirely. For those types of actions the audit committee may well want to pull individuals from the IT department and the internal audit department to function as special investigators for that action. This may be particularly required where physical and logical access controls must be bypassed with the assistance of individuals within the IT department so that whistleblower investigators can conduct their examination.

Another consideration about the structure and management of the self governance program is when to consider the use of outside experts. Computer forensics have been selected as a tool for responding to whistleblowers and monitoring internal control because of its acceptability in court. If this is a matter that will be proceeding as a legal matter, then the use of an outside experts is essential. In the event of a legal proceeding, it makes no difference how expert the organization's personnel actually are, they will always be either plaintiff or defendant. Thus, they can never be an expert. So, as part of the structure and management of the self governance program it is only appropriate that a threshold be established for when to obtain an expert.

A discussion of structure and management would not be complete without a discussion of additional internal controls. Computer forensic tools are very powerful and often allow users to by pass elements of the organization's physical, logical and application controls. Other physical, logical and application controls, however, could require the assistance of their administrators. Consequently, appropriate consideration should be given to both the tools that will be used in a computer forensic investigations as well as the segregation of duties that is required to prohibit their unauthorized use within the organization. Indeed, computer forensic tools may need to be used only by internal auditors who are working on authorized projects in concert with IT personnel who have allowed the auditors to bypass physical and logical controls so that those tools could be used.

## Resources

After deciding on a structure, the next question becomes what resources will be required? Naturally, the answer to the question about resources includes both personnel as well as forensic tools. With regard to personnel the organization should obtain adequately trained individuals. Individuals with computer auditing backgrounds and certifications are a likely consideration.

Computer auditing is a significant part of the internal auditing field. Consequently, internal auditors are an appropriate choice. In addition to their experience and expertise with computer auditing, they would also have the disciplines for investigating, analysis, report writing as well as the unique interpersonal skills required for this type of work.

IT personnel are another logical choice, although there is a dramatic difference between operating a system and investigating one. Conceptualization skills, skepticism, the analytical ability to find weaknesses, and the creative skill to adequately test hypotheses are important skills for the investigator. Similarly, there are other contextual limitations from which IT personnel may suffer. The Enron debacle involved a flawed accounting concept. The Worldcom debacle involved improper capitalization of periodic expenses and many of the other financial disasters involved inappropriate revenue recognition methods. Thus, while an IT person may have the necessary computer skills to evaluate security policies, the ability to apply those skills to business disciplines such as accounting and internal control and recognize the significance of evidence discovered is another matter. Yet the reality is that the IT department is the manager of the organization's computer resources. Thus, they will be the first layer of internal control. What should not be underestimated is the importance of the second layer that resides outside of the IT department.

As stated previously, the analysis of a whistleblower complaint may, in fact, require coordination of IT and internal auditors. Complete investigations will require that normal internal controls (in the form of physical, logical and application controls) be bypassed so that the investigator can collect his evidence and perform his analysis. Thus, segregation of duties requires that both the IT department and internal auditors work together.

In addition to picking the right personnel, the personnel selected should be adequately trained. Organizations may want to use education and professional certifications as a basis for staff selection. Computer science and information system degrees can be beneficial but these are still relatively new educational curriculums and there still are many seasoned professionals who have developed their skills through many years of practical experience. The same can be said for professional certifications. There are a few that have long histories. Certified Internal Auditors (CIA) and Certified Information Systems Auditor (CISA) are professional designations with maturity. Other disciplines such as computer forensics are young and still evolving. Yet, designations like Certified Computer Examiner (CCE) and Certified Information Systems Security Professional (CISSP) do exist and can be discriminating factors in personnel selection.

After the personnel are acquired they will require sufficient tools with which to perform their analyses. Earlier in this writing numerous tools were identified. There is no single tool that will enable the organization to adequately perform this function. A collection of tools will be required,

however, such as write protection devices, imaging and other preservation tools, and analysis tools. In addition, to the computer forensic tools organizations may want to consider other software resources such as Enterprise Content Managers and Enterprise Records Managers and third party monitoring software that records employee activities and tracks usage of trade secret information.

## Methods

The methods that can be employed are essentially of two different types; reactive and proactive. Reactive, methods involve incident response triggered by either whistleblower complaints or detective alarms that signal a potential breach in internal control. Incident response essentially involves those methods for preserving evidence described in the initial section of this writing and then analyzing the data collected with the appropriate tool or tools. A few of the different tools were also discussed in the first section of this writing.

As to the particular methods that should be employed, a few of the standard analyses are identified in the following list.

- Examination of the file system contents and usage patterns.
- Recovery of deleted files.
- Signature analysis to detect mislabeled files.
- Hash analysis to determine digital fingerprints, identify duplicates and previously identified but prohibited software and data files.
- Registry analysis to determine users, mapped storage locations, previously installed programs, hardware and other components that might not be currently observable from the examination of the file system.
- Examination of LNK files to spot other data storage locations and determine recent usage activity,
- Review of application, security and system event logs for activities warranting additional investigation.
- Examination of internet search and browsing activity.
- Recovery and examination of e-mail messages and attachments.
- Reconciliation of logical storage areas to physical storage capacity.
- Examination of protected areas for hidden data.

- Examination of free space.
- Examination of hidden data or data otherwise protected by passwords, encryption, etc.
- Search for signs of obfuscation.
- Search for terms and other signatures of potential evidence.
- Review and evaluate other repositories for internal control information such as network logs, etc.
- Evaluate extension of the investigation throughout the network and determine the scope for expanded examination.

The proactive methods are very different from the reactive methods. They are not in response to any incident but rather are part of the review and evaluation of internal controls. They could encompass a variety of methods for evaluating physical, logical and application controls. With respect to computer forensics, those techniques would be used to monitor the review and evaluation of the internal controls at a low level to ensure that they were working as designed. Such tools could include:

- Disk editors to examine the exact changes to storage media as physical, logical and application controls are tested;
- Memory and disk monitors to review programs effected and the changes made to storage media as physical, logical and application controls are tested;
- Port watchers that look for signal communications as physical, logical and application controls are tested;
- Packet sniffers that review the contents of signals transmitted to determine that they are as expected as physical logical and application controls are tested, and finally,
- Enterprise applications that enable stealthy searches and live analysis of remote systems over the network for installation of prohibited software, improper settings, malicious software, covert communication channels, prohibited computer usage, prohibited data, forensic grade media imaging, etc.

## Conclusion

The Sarbanes-Oxly Act of 2002 was designed to protect investors by improving the accuracy and reliability of corporate disclosures that are made pursuant to securities laws, and other purposes. In order to facilitate the accomplishment of these objectives, the Act made numerous changes. Three of those changes were:

- The imposition of penalties for the destruction, alteration or concealment of documents including computer data;
- Requiring the signers of financial reports to design, install and maintain internal controls adequate to ensure the accuracy and integrity of those reports; and
- Directed whistleblower resolution practices and provided whistleblower protections.

Since so much of an organization's systems and data are computerized, the use of computerized tools will be essential in satisfying the requirements of the Act. One of the tools that is well suited for responding to whistleblower complaints and strengthening internal control is the computer forensics.

With respect to whistleblower complaints, computer forensics will be essential in preserving, analyzing and presenting evidence that either supports or refutes a whistleblower's claims. If the matter proceeds to court, computer forensic techniques will be essential in settling the dispute.

Responding to whistleblower claims is not the only role for computer forensics, however. As stated above the Act places more importance on the role of internal control. Computer forensic techniques can be very useful in monitoring the effectiveness of internal controls as well as functioning as an internal control mechanism.

When actually implementing the self governance program necessary to ensure compliance with the Act, the use of computer forensic techniques will likely be found in three layers of the organization's control structure. Certainly they will be used for the evaluation of whistleblower complaints. They will also be used by management, particularly the IT department, as an internal control mechanism. The third layer will likely employ the use of computer forensics as part of the internal audit function and the independent assessment of management's physical, logical and application controls of the computer infrastructure.