

# What to do when your office is a crime scene

Your company has done everything your accountant told you, setting up a strong internal control system. Your annual audit or review resulted in a clean bill of financial health.

But that trusted employee was untrustworthy.

Your offices have now become a crime scene.

You don't know where to turn. The actions you take may be the difference between whether or not you recover any of the proceeds of the crime.

Your actions may keep your company from suffering further. And your actions could make the difference in whether you go to jail. What must you do?

First, be sure the employee no longer has access to your company's information system and office space. The employee's passwords must be deactivated to deny access to your information system.

As a general rule, the employee should not be allowed to return to the premises during an investigation, even if the employee is cooperative in the investigation.

But equally important, you should not examine the employee's computer nor search his office.

This is the equivalent of placing yellow tape around a murder scene. These activities, as well as interviews of employees, should be undertaken only by trained professionals.

These professionals know how to find and properly preserve potentially incriminating evidence. Proper evidence handling can be the difference in your recov-

## Our View

Donald H. Minyard  
& Alton Sizemore Jr.

already have one, you will likely need to hire an attorney.

Don't fire the employee without advice. Your attorney needs to coordinate and monitor the activities of internal and external investigators.

Your communications with your attorney are privileged, as are your attorney's communications with consultants such as forensic accountants.

It is very unlikely your current accountant should service your investigative needs. The accountant who does your taxes or financial statements is apt to have a conflict of interest in forensic matters.

An accountant with whom you have a continuing relationship is not likely to be independent of the situation being investigated. That may be important when the matter heads to court.

Once the investigation gets started, you will need to have appropriate hard drives mirrored by trained professionals (in other words, like they say on TV, don't try this at home).

The original hard drives need to be set aside and protected as evidence. Mirroring makes a copy of the hard drive as it existed on the date imaged.

Making the mirror image allows examination of the copied hard drive without

erling economic losses suffered.

After securing your facilities, the process gets more complicated.

If you don't

disturbing the data that exists on the original.

This is important because you don't want anyone accusing you of changing or deleting any of the information on the drive.

During the examination, a forensic data examiner will look for documents, e-mails and images, as well as files that have been changed or deleted.

The dates and times of deletions or changes can be invaluable in the process of determining who did what and when and why they did it.

One area that may be of particular interest is metadata, which is information about the data in a document or other file.

Reviewing metadata can explain changes in files – the who's, when's and what's of occurrences being investigated.

Knowing these, a forensic accountant then can help determine the why's and how's of financial crime. Because of this, it is vital to the investigation that the forensic accountant communicate document needs to the data examiner.

You also need to know what to do when the data examiner finds information you have not anticipated.

Many companies have learned of employee involvement in illegal activities not related to the company (for example, downloading child pornography).

These illegal activities may impact the company, as criminal investigators may seize the company's computers as evidence of the unrelated crimes.

Finally – and in the post-Enron world

***Failure to obey laws involving evidence preservation can make you just as guilty as the offending employee.***

this should go without saying – do not destroy evidence. This means computer data as well as hard copies.

The requirement to avoid evidence destruction underscores the importance of the roles of professional investigators.

Failure to obey laws involving evidence preservation can make you just as guilty as the offending employee.

If you destroy evidence, you could possibly be convicted of crimes such as conspiracy, obstruction of justice or impeding an investigation. Convictions of these crimes can result in prison sentences.

This article has outlined the steps you must take immediately when you discover your office is the crime scene. Be sure to engage the services of competent help, so that you don't become a victim of your own mistakes.

**DONALD H. MINYARD and ALTON SIZEMORE JR.** are fraud examiners and forensic accountants with Summerford Accountancy PC, a nationally recognized forensic accounting firm. They can be reached at (205) 716-7000 or don@summerfordcpa.com and alton@summerfordcpa.com.