Anti-Fraud Controls in a Weak Economy

Almost every day of the week you will find a newspaper article about a former employee being indicted and/or convicted of embezzlement. The common thread across all of these stories is usually:

1. They were the “trusted” employee,
2. They were like a member of the family,
3. They were outgoing and personable to the boss, outside vendors, customers, and decision-makers,
4. They were extremely protective of their “own turf” and kept other employees away,
5. They would not share their duties, and often they worked longer hours than anyone else in the company,
6. They had a “monkey” on their back.

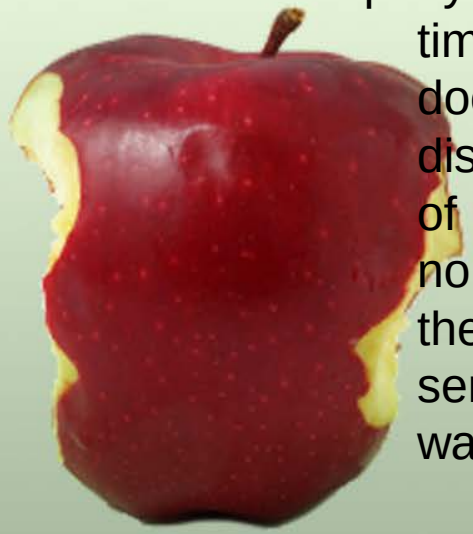
The care and feeding of monkeys….

What is a monkey?

- ❑ An economic dependency – gambling, drugs, bad investments, family members that demand support, and other activities that take more from the relationship transaction than they give.
- ❑ A social dependency – bad relationships with spouses, ex-spouses, significant others, children, and friends.
- ❑ Living above one's means – keeping up with the Smith's.
- ❑ Status and social class – feeling that they are due more and should not have to earn that achievement.

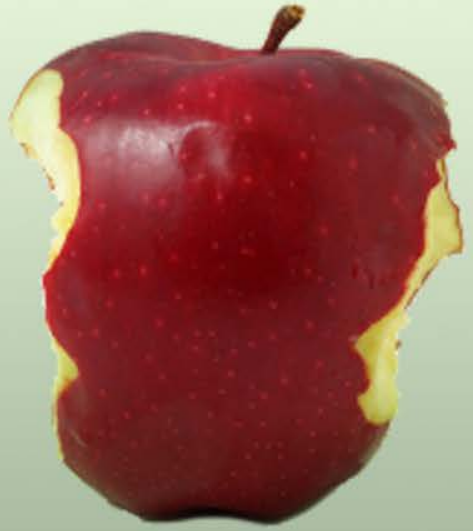
Why it pays to know….

In the late 1970's I was in charge of operations of a Houston area bank. One day a teller brought a suspicious deposit to my attention. The deposit consisted of a series of escrow account checks issued by a large title company in the city. Each check had a different payee and a second endorsement. Every check had been deposited in the checking account of an elderly woman who would come in the bank fairly often accompanied by her old dog. Within a day I had checked microfilm records; identified five other banks that were being used, and identified a senior vice president at the title company who had signed every check. Over a seven year period of time, which was as far back as our records went I was able to document approximately $800,000 in losses. All of the disbursements were from an escrow account which consisted of left over funds from real estate closings. Customers had no idea that they were due funds and only one person with the title company was in charge of this bank account – the senior vice president. When I contacted the title company I was met with incredulous disbelief.



She was the trusted employee….

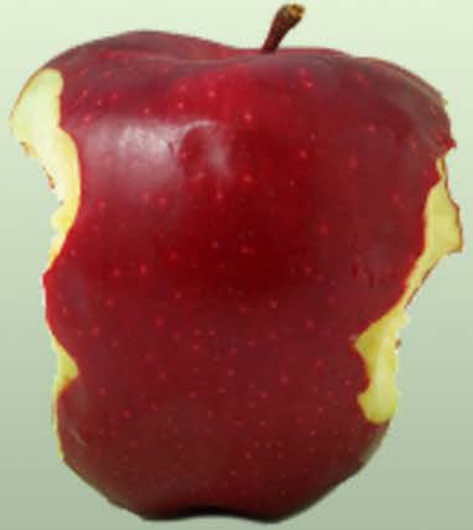
The title company executive related to me that the SVP was held in the highest esteem in the company, and that she had, in fact, trained him. After being presented with the name and a picture of our bank customer, and her dog, the executive stated that she was the former secretary of the SVP. Further probing resulted in him telling me that the secretary had been injured in a fall at work, and that there had been some issues with respect to disability and her retirement. When I questioned him about the lifestyle of the SVP he related that she lived in a large house in West University near Rice University; she would host fantastic Christmas parties every year for the company, and that he believed that her husband was very successful in the oil and gas industry. Meanwhile the secretary was living in a "cracker-box house" on the north-side of Houston. For the reader the real truth is obvious – lies, all lies. When the judge sentenced them, he gave them each probation because of their ages, and made them convey title to their homes to the title company. They were allowed, however, life estates in their homes.



Lessons from the poisoned apple….

Observations from this case are defining moments for all fraud investigations:

- Fraud is rarely discovered by external or internal auditors. Neither one of these groups when contacted by me had a clue of what had been going on.
- Fraud is frequently discovered completely by accident and is often a matter of pure luck.
- Segregation of all duties in the hands of one “trusted employee” encourages fraud, an increase in the monetary amount of losses, and the duration of fraud.
- Collusion normally results in larger losses.



- Disgruntle ex-employees represent a significant threat when grievances are not appropriately addressed. Current employees will often feed on that anger, or allow themselves to be used because they feel their employer hasn’t done the right thing.
- The full extent of losses often cannot be determined because business records have been destroyed, an adequate records retention policy is not enforced, or the employer that suffered the loss does not want to publically admit that they were taken.

Rocket science and fraud….

In every financial transaction there is an element of trust, and a bond of faith that the other party will do what they say they will do. In turn that employee, customer, or vendor believes that you will do what you say. People that commit fraud (fraudsters) frequently display the following patterns:

- ❑ Fraud is often rationalized with mental phrases such as – *"it's just a loan, I'll pay it back soon." "I deserve it more than they do,"* or *"You know they've been stealing from the company for years!"*

Regardless of the dynamics you can usually count on a handful of factors:

- ❑ The majority of frauds are never identified and when identified are frequently not prosecuted.

- ❑ Most fraud is simple, straight-forward, and does not represent a high degree of sophistication. It represents a crime of opportunity, but clearly is planned.
- ❑ A large number of people who commit fraud are serial-fraudsters. They have committed fraud or some other type of property theft in the past, but have not been caught, weren't prosecuted, or their current employer failed to do an adequate background check.
- ❑ Employers have deliberately circumvented internal controls thereby making fraud easier.

More dynamics of fraud….

- ✓ Fraudsters are usually extremely likable. They are often friendly, engaging, and willing to please. You will experience more "personal and emotional damage" when you have to bust them than they will feel. You have been used and while you have been violated, their feelings often tend to be generalizations or rationalizations. Tears frequently follow on their part, but that reaction is normally – *"I'm sorry I was caught,"* not *"I'm sorry I did it."*

✓ Fraudsters usually look upon their acts as white collar, non-violent crime that is victimless. This allows them to divorce themselves from the nitty-gritty reality that material fraud really does put companies out of business, and that there are indeed victims.

✓ In a bad economy the number of occurrences of fraud increases, but, as a rule, the number of discoveries of internal fraud decreases. This is usually attributable to internal controls being reduced as the number of employees is cut.

✓ Investigative resources are also cut and the deterrence factor is reduced.

They call it extortion….

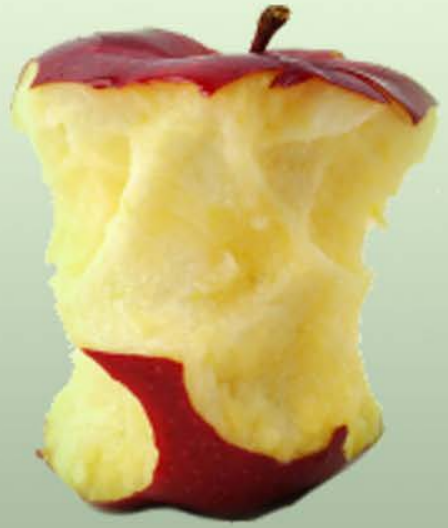
Guilty people can do very bad things when they are on the verge of getting caught. In recent years the incidence of physical violence has increased when frauds were discovered. This may be attributable to the large sums of money that can be embezzled from small businesses now, less tolerance of white collar crime in the judicial system, tougher government regulations in some industries, or a cultural phenomenon which results in a greater tendency to resort to violence. This highlights the fact that suspected fraud should not be investigated by amateurs:

- Conflicts of interest – must be avoided. Investigators must be independent of the company, the management, shareholders, customers, and employees.
- Specific knowledge of fraud – investigators must be specially trained and proficient in the identification of fraud.
- Industry knowledge – many types of fraud are industry specific and investigators must know the industry well.
- Self-investigation – often results in contaminated evidence, chain of custody issues, and an inability to prosecute. It should be avoided at all costs. This is not a DIY area and legal disasters can occur very quickly.

It’s all in the computer….

There are an alarming number of companies that fit the following pattern:

- Inadequate segregation of duties – accounting personnel wear several hats. It is not usual to find an office manager/bookkeeper who posts cash receipts, prepares deposits, posts the general ledger, reconciles bank accounts, and pays bills. One way or another the central “trusted employee” has significant control over the cash receipts cycle, the cash disbursements cycle, and all financial reporting.



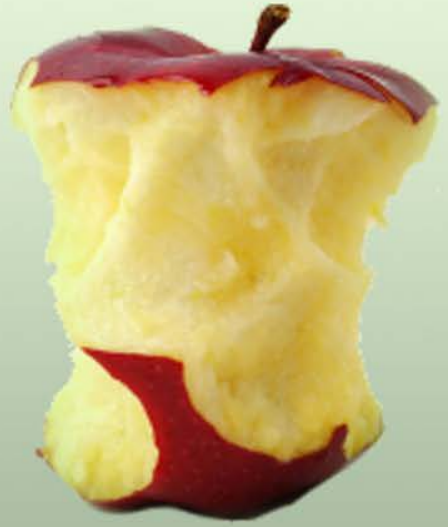
- Accounting software is inadequate – with insufficient program controls, poor documentation, backdoors, and easy data manipulation. Audit trails are insufficient.
- No IT manager – security updates are not adequately maintained, firewalls are obsolete or the software subscription has expired, and Internet access is not adequately controlled, monitored, and documented.
- No privacy policy – the company lives in peril because it does not understand the legal issues inherent with digital access.

Digital forensics and evidence….

Almost everything that we do in today's society is chronicled in the form of digital evidence: (1) access to our PC at work or at home, (2) remote access to a server at work, (3) internet browser activity and history, (4) music, movies and other media we download on our PC or gaming device, (5) cell phone records including calls made, calls received, texting activity, apps downloaded, and our physical movements, (6) waypoint information from vehicle GPS devices, (7) black box data recorded by car computers, and (8) scores of public and private data collection devices that record thousands of individual data records that document what we buy, when we buy it, where we travel, what we drive, how fast we go, and when we get there. Any reasonable expectation of privacy is in a very real sense mythical, but that does not mean that as an employer that you have a right to trample on the constitutional rights of an employee expected of wrong-doing. On the other hand this evidence is fleeting in nature, easily subject to change, corruption, or contamination, and is extremely hard to present in court.

Who is qualified to do digital forensics examinations….

Three states in the United States (Illinois, Michigan and Texas) specifically require a private investigators license in order to perform a digital forensics examination. There has been a substantial degree of misinterpretation, and in some instances misrepresentation, of this statute which is contained in Chapter 1702 of the Texas Occupations Code. In actuality, public accounting firms and CPA's properly licensed in the State of Texas under Chapter 901 of the Texas Occupations Code are specifically exempted under Chapter 1702.324(b)(14) Certain Occupations from the requirement to have a private investigators license in order to perform digital forensics examinations. That said, our firm only performs digital forensics examinations under the engagement letter of an attorney because:



- Accountant-client privilege is recognized in state courts in Texas. It is not recognized in federal courts.
- A CPA must be under the "umbrella" provided by attorney-client privilege in order to maintain the confidential nature of their work, and their work may not be subject to discovery if they are a non-testifying expert.
- These are very "thorny areas" and it requires careful coordination between CPA's and appropriate legal counsel.

Developing an emergency response team….

Fraud is often exacerbated because management doesn't know how to properly and objectively analyze what is happening. The simple truth is that fraud is much the same as a natural disaster – it can have long-term, lasting effects like fire, flood and wind. The magnitude and duration of damage is mitigated by having emergency plans in effect long before disaster strikes. Knowledge of these policies can constitute an effective deterrent for employees. At a minimum the following should be included in a fraud response policy:

- Management of IT Resources (server) – offline mirror imaging of server hard drives within the first 24 hours of the discovery of internal fraud; physical control of all back-up resources; termination of offsite access through virtualization software and remote terminal software; capture of all log files; and identification of applications and data files that may have been compromised. Establishment of the chain of custody and the control of evidence.

Identifying damage….

Often the first thing that business owners and senior managers want to do when fraud is discovered is to play the "blame game" and start pointing fingers. Experienced fraudsters count on this, and alienation of good employees and outside professionals can often result in any chance of criminal prosecution and recovery of assets getting thrown out the window.

- Management of IT Resources (workstation) – all PC's on and offsite that may have been used to commit the fraud must be physically controlled, taken offline, and turned off. For practical purposes the data on these computers is equivalent to murder weapons. Allegedly a crime, or a series of crimes, have been committed and the proving of guilt or innocence may be located on the hard drive, a backup drive, a thumb drive or another digital storage device.

- Imaging of Digital Media – this should be done immediately after the suspected fraud is discovered. This should only be done by a qualified digital forensics examiner that has met appropriate educational and experience requirements.
- Change of Custody – four images of suspect hard drives should be made. (1) Company attorney, (2) Law enforcement, (3) Digital forensics examiner engaged by the company, and (4) Defense attorney. All hard drives should be appropriately controlled under dual control in a fireproof safe until they are distributed under legal agreement. The original suspect hard drives should be controlled by the company's attorney until they are turned over to law enforcement. Documentation of hashes should be confirmed before distribution.

This isn't NCIS….

As a rule district attorneys don't understand very much about digital evidence. What they do understand very well is the necessity to maintain a proper chain of custody of evidence, and the absolute imperative to avoid the contamination of evidence. While I dearly love Abby on NCIS, and I dream of her autographing my write-blocker, don't think for a moment that you can replicate "forensically-sound" investigative techniques in your office. It won't happen and before you let just anyone near that suspect computer do your homework!

✓ Engage an Attorney who Understands Digital Forensics – they should understand technical concepts well and should be comfortable with presenting digital evidence in court.

✓ Engage a Digital Forensics Examiner – that meets appropriate educational and experience requirements. They should have substantial experience as an expert witness and they should be well-versed in computer science, fraud investigations, forensic accounting, and legal procedure.

✓ Avoid DIY – don't contaminate the crime scene and don't let "amateurs" take charge of your investigation. Only hire seasoned professionals that understand all phases of the problem at hand.

Conclusion: Controls vs. Trust….

1. CPA's must consider the possibility of fraud – when performing a financial statement audit CPA's must consider the likelihood of fraud, but they are not specifically trained to identify and investigate fraud. Only a handful of colleges in the United States provide accounting electives in forensic accounting and fraud auditing.
2. Audit tests – are not specifically designed to test for and identify the presence of fraud.

3. Internal controls – provide the most cost-effective solution to mitigating fraud risk.
4. Background checks – must be done for all applicants in positions of trust, as well as outside professionals and independent contractors that do significant work for the company.
5. Bond and fiduciary coverage – insurance coverage must be comprehensive and more than adequate to cover any anticipated internal fraud.
6. Digital forensics – must be considered in investigating and documenting any suspected fraud.

Our qualifications….(in a nutshell)

Hugh E. Gardenier, III – CPA (State of Texas 1980), CFE (2008), CFF (2010); MS in Digital Forensics – Sam Houston State University (2010), MS in Accounting – University of Houston (1981), BBA in Accounting – University of Houston (1975)

Member of AICPA

Forty years of accounting and auditing experience. Two years in internal auditing; three years in bank operations, and thirty-five years in public accounting.

Martha L. Gardenier – CPA (State of Texas 1992), CFE (2008), CFF (2010); MS in Digital Forensics – Sam Houston State University (2010), JD – South Texas College of Law (1998), BBA in Accounting – Sam Houston State University (1990)

Member of AICPA

Thirty-nine years of accounting and auditing experience. Thirteen years in real estate accounting, computer services, oil and gas, and beverage distribution. Twenty-six years in public accounting.

Gardenier & Associates, PLLC
Certified Public Accountants
2 North Hornbeam Place
The Woodlands, Texas 77380
(281) 923-9853 fax (281) 363-3573

mailto:sma69@msn.com