Forensic Focus

Insights on fraud detection and deterrence

OCTOBER/NOVEMBER 2008

Your computers might be at risk …
from your employees

Would you know
insurance fraud if you saw it?

Why people cheat
Almost anyone could become a fraud perpetrator

Walkthroughs still matter

Two things are inevitable: Fraud and taxes

McGOVERN & GREENE LLP

CPA's & Forensic Accountants

105 W. Madison Street • Suite 406 • Chicago, IL 60602
www.mcgoverngreene.com

Your computers might be at risk … from your employees

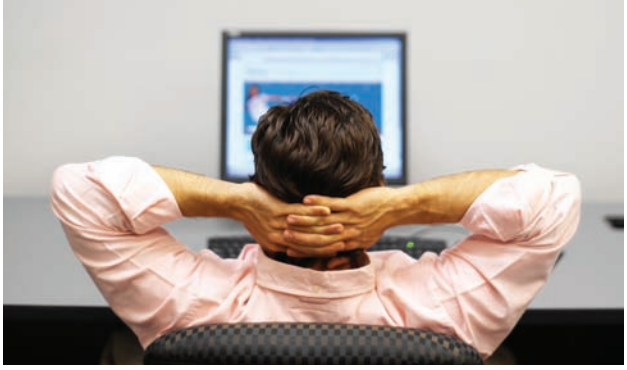
You use firewalls and encryption to protect your business's computer system from outside predators, but do you guard against the fox that's already in the henhouse? Employee computer crime is a real threat, and you must consider its possibility in your fraud-prevention program.

No skills required

Internal computer fraud can include any of a number of transgressions, from illegally copying software to stealing trade secrets to outright theft of company equipment. It can occur at any point in the system: data input, software, data storage or data output.

The input stage, however, typically offers the easiest means for theft. Someone stealing inventory, for example, can update the system to indicate the inventory has been scrapped. The action requires no particular computer skills; the perpetrator just needs to know how your system works. It may be a little harder to damage or change stored data files, but a determined employee with some advanced knowledge of your system can do it. And anyone with access can copy or print output.

Virtually every employee is probably using your system for personal reasons, whether to pay bills, shop for birthday presents or send personal e-mails. Unless such activities are consuming an inordinate amount of time, you probably regard them as benign. Most of the time that's true, but there are exceptions: If an employee is sending sexually harassing e-mails through the company system, for example, you may be legally liable.



Be a culture vulture

The problem is that employees must use the system to keep your business going. And to do that effectively, they must know how the system works. The challenge, therefore, is to give your employees all the knowledge they need to perform their jobs and, at the same time, prevent them from using it against you.

One way to do this is to create a business culture that's hostile to fraud by:

- Identifying areas of greatest risk,
- Creating ethics policies,
- Stressing integrity at all levels of the organization, and
- Ensuring that all employees are effectively supervised.

In addition, when you train your employees in computer usage, instruct them in security and fraud prevention as well.

Take control

More practically, develop a strong internal control system for your IT network. At its most basic, this means segregating duties and restricting access to system resources. But you also must monitor servers, back-ups, e-mails and Internet activities. Employees may experience a small loss of privacy, but you own your company's computers and networks, and you have the right to protect them. Just let employees know up front that you'll be randomly monitoring their computer activities and that you regard monitoring as a routine part of doing business.

Perhaps the most important strategy to protect against internal computer fraud, though, is to know who has access to what data and how that access is controlled. If you have your own server, keep it in a locked room and log everyone who enters and exits.

Require employees to have passwords for their computers and for particularly sensitive files stored on them. To be effective against intruders, passwords should be complicated. They should include numbers and upper- and lowercase letters, and they should be changed frequently. Also be sure to warn employees against writing them down and leaving them in a readily accessible location — such as taped to their monitors.

Lock the back door

Keep in mind, too, that disgruntled or recently fired employees can use purloined passwords to gain remote access to your company's network. Once in, they can do untold damage by adding, deleting or altering files.

If you must let someone go, be sure to disable his or her access authorizations immediately, and require everyone in his or her department to change passwords. You might also ask your systems administrators to check the files and systems to which the departing employee had access. Employees who sensed their firing was imminent have been known to install programs that will delete files after they've left.

Don't make it easy

As you consider which safeguards to use in protecting your computer system from internal fraud, remember that your objective is to make it harder and riskier for anyone to go where they don't belong and to make it less rewarding if they do.

An accounting clerk with the skills and knowledge required to create false vendor accounts, for example, might be less tempted to attempt such fraud if colleagues always lock unattended computers and are careful to keep their desks and monitors clear of sensitive information. And the employee is likely to think long and hard before attempting a fraud that could lead to unemployment or criminal prosecution.

If your company has an anonymous hotline or other fraud reporting mechanism, make sure it's well publicized that you investigate all tips. If you don't have a hotline, consider getting one. It may be just the thing to prevent a payroll clerk from handing out unauthorized raises.

Recognize a real threat

Obviously, you need to protect your computer systems from external security threats, but it's important to recognize that the greatest threat may come from within. Even your most trusted long-term employee is a bigger risk than a hacker. He or she is a fox that knows not only where the hens roost, but also where they lay their eggs. ■

Would you know insurance fraud if you saw it?

Insurance fraud has a timeless appeal among scam artists, but it becomes even more popular when economic times are hard. Slip 'n falls, fake car accidents and even arson are greater threats as people feel a pinch in their pocketbooks. So now is a good time for businesses to redouble their protection and recognition efforts.

Be skeptical

Slip 'n falls are among the most common insurance scams, and they can lead to big payoffs. Consider the case reported several years ago by Federated Mutual Insurance Company. A pregnant woman stated that she'd slipped on a wet sidewalk outside a

business and that the resultant fall caused injuries that ultimately led to a miscarriage.

The woman claimed that the business's owner had failed to maintain the premises properly or warn her of the danger. She provided an emergency room report verifying the miscarriage and demanded a $60,000 settlement. But when the insurance company ordered her medical records directly from the hospital, there was no mention of a miscarriage. She had rewritten the report, and her claim was denied.

A security camera system can help you monitor activity on your premises and capture critical evidence of fraud.

But there are plenty of ways to perpetrate insurance fraud. For example, three generations of a Los Angeles family bilked insurers of millions of dollars for injuries and collision repairs from fake auto accidents. And a Connecticut man torched his own car and then reported it stolen to claim the insurance money.

Be observant

Too often, insurance fraud succeeds because there's no reliable evidence to prove it. You can protect your business from premium hikes and litigation by being aware of the potential for these schemes.

A security camera system can help you monitor activity on your premises and capture critical evidence of fraud. But as with other types of occupational fraud, your employees are your company's first and best defense. If an employee is faking an illness or injury to collect unmerited worker's compensation, his or her co-workers probably will be the first to know. If a fire in your warehouse was set intentionally to hide missing or stolen inventory or to help the department recover from a lackluster quarter, employees who worked there may be suspicious before you are.

Be detail-oriented

Train employees to respond properly to potential fraud incidents so you don't lose important information. If there's an incident on your property, employees should photograph the accident site immediately, and then collect and document specifics such as the:

- Name, address, phone number and date of birth of the injured person,
- Date, time and location of the accident,
- Weather conditions at the accident site (if outdoors),
- Nature of injuries reported by the victim,
- Names, addresses and phone numbers of witnesses,
- Description of the accident and how it happened, and
- Description of the injured person's appearance and attitude.

As well as informing you, employees need to report accidents or emergencies to your company's insurance carrier immediately. They should also relate any suspicious behaviors or comments that might lead them to believe the incident involves fraud.

Eyes wide open

Employees generally don't like to "rat out" their fellow workers. So be sure to give them a safe way, such as a confidential hotline, to report their suspicions. And include common insurance scams and their warning signs in your company's fraud prevention program. These simple acts could protect you from some major headaches and worse — financial losses. ■

Why people cheat

Almost anyone could become a fraud perpetrator

Wouldn't it be nice if people prone to fraud had the letter "F" stamped on their forehead? You could monitor them closely and make sure they never had access to the accounting books or other sensitive information. Unfortunately, potential fraudsters are never that obvious.

Everybody loves a cheater

In many cases, employees who commit fraud are the most likable people in the office — personable, helpful and good at their jobs, as well as seemingly trustworthy. But fraud doesn't begin with dishonesty; it begins with pressure. The pressure may be internal (corporate demands to meet revenue goals) or external (a desire to keep up with the wealthier Joneses), but it's strong and unrelenting.

In some cases, ego is a powerful motivator. The ability to put one over on the boss or the company or to control other people is more rewarding for some than the actual proceeds of the fraud.

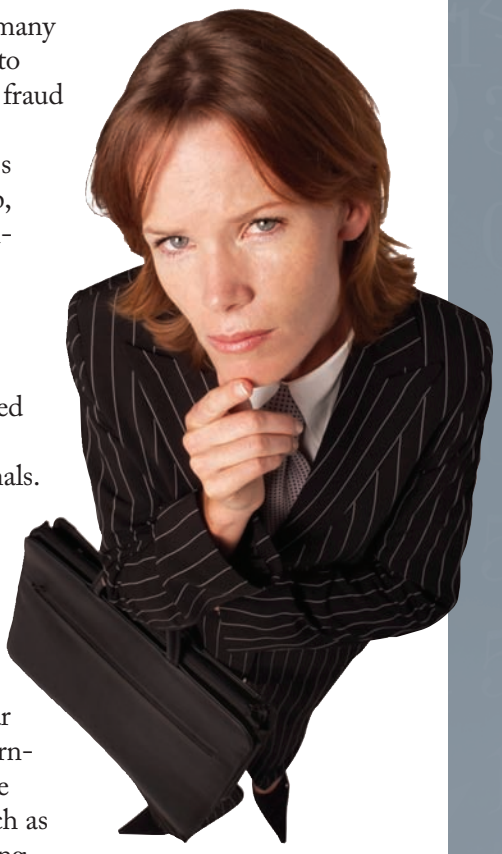
Upper-level fraudsters may be extremely ambitious and have an overdeveloped sense of their own superiority. These individuals are likely to be unreasonably sensitive to criticism or scrutiny and to surround themselves with sycophants.

Rank-and-file employees who commit fraud, on the other hand, are more likely to feel they've been treated unfairly and steal to seek retribution. They may also develop a sense of territorial ownership of the company's resources — "my computer" or "my budget" — and, thus, feel justified in taking them for personal use.

Another, and fortunately less-common, type of occupational fraudster is the thief who can lie to people's faces and leave them penniless without remorse. These con artists are similar to the criminals who bilk little old ladies of their life savings, and then castigate the victims for being stupid.

What, me worry?

Blaming the victim is, however, a fairly common way for fraudsters to justify their activities to themselves. Whether they have a sense of entitlement or believe their employers can afford the financial losses, scammers find ways to distance themselves from feelings of guilt.



The trouble is that many of the skills needed to successfully commit fraud are also necessary to thrive in the business world. Salesmanship, sociability, determination, persistence, competitiveness and a desire to obtain material possessions all are frequently cited as characteristics of successful professionals.

Some people with those attributes will commit fraud in a given situation, while others can withstand similar pressures without turning to fraud. In some environments — such as companies with strong internal controls — fraud is too risky for virtually anyone to attempt. In more-lax environments, anyone might be tempted simply because it seems so easy.

The science of fraud

Research has yet to firmly identify the psychological indicators of fraud and make it easier for companies to spot dishonest employees before they commit a crime. But there are plenty of effective tools to keep occupational fraud in check — starting with

aggressive pursuit and punishment. Publicity and imprisonment are likely to be more devastating to white-collar criminals than to common street thugs. Indeed, as the likelihood of exposure increases, the likelihood of fraud decreases.

For similar reasons, a strong antifraud environment may be highly effective in keeping occupational fraud at bay. A culture that encourages honesty and fairness makes it that much more difficult for fraudsters to mentally justify their activities.

Cultivate integrity

The behavioral warning signs of fraud may not be as obvious as you'd like, but keeping them in check is easier than you may think. Trust and value your employees, but at the same time, don't make it easy for them to commit fraud. ■

Walkthroughs still matter

You've got internal controls to fraud-proof your company's checks. Every check requires two signatures, and one of them must be yours. Sure, you have a signature stamp to make the job easier on your hand, but it's locked in your office when you're away and no one has access besides you.

And yet, fraudulent checks have been getting through for months. An expert walkthrough of your controls reveals that a trusted manager with heavy gambling debts has a master key and has been stamping checks with your signature.

No skipping allowed

Under Auditing Standard No. 5 (AS5), issued last year, public companies are no longer required to hire auditors to conduct a walkthrough — or trace a transaction through organizational procedures from start to finish. They must, however, still achieve all the objectives of a walkthrough by ensuring that the company's staff performs one.

But for both public and private companies, a walkthrough is still the best and most efficient way to identify weaknesses in procedures and controls. Although AS5 allows auditors to supervise employees or a third party who performs the actual walkthrough, it may not be as effective as an auditor-led walkthrough. Your staff, for example, may not be able to approach the process with the same level of objective assessment that an auditor could. Auditors might ask employees to explain why they perform a particular step in an operation. Employees, on the other hand, may believe they already know the answer and therefore never bother to ask the question.

Still the best

Although AS5 gives auditors more leeway in deciding how to conduct walkthroughs, it also codifies the need for a risk-based approach to audits. This means they should be more focused on identifying control weaknesses and potential loopholes that fraudsters can exploit.

So even though auditors are no longer required to conduct walkthroughs themselves, walkthroughs may, in fact, be more important than ever. If nothing else, walkthroughs can reveal inconsistencies that might otherwise go unnoticed. One accounts receivable employee may believe errors are to be handled a certain way, for example, while another interprets the instructions differently and uses an alternative technique.

Different approaches

AS5 represents an opportunity for companies and auditors alike to take a new look at an old tool. Different companies may prefer different approaches, but walkthroughs are likely to remain one of the best defenses against fraud — for everyone.

Two things are inevitable: Fraud and taxes

Just when you think you've heard it all, fraudsters come up with another way to separate you from your money. The newest ruses use the name of the IRS — and they're very convincing.

Dialing — and phishing — for dollars

In one of these new schemes, someone posing as an IRS employee phones fraud targets and tells them that they're eligible for tax refunds as rewards for filing their taxes early. But there's a catch: The thief claims that refunds are available only through direct deposit. If a target isn't willing to provide bank account information for the "deposit," he or she won't receive the refund.

A similar scam uses e-mail to offer specific refund amounts. Targets might be asked to click on a link to a claim form that requests personal information. Scammers then use that information to access bank or credit card accounts. And in many cases, targets are directed to authentic-looking Web sites that request recipients' mothers' maiden names as well as their birth dates and Social Security numbers.

In a newer version of the scheme, scammers e-mail notifications that tax accounts will be audited. Unlike most fraudulent e-mails, these messages may be personalized to recipients and appear very authentic. But they still request personal and financial account information that the fraudsters use to conduct identity theft.

Corporate victims

Businesses aren't immune to these schemes. Scammers have been known to send e-mails to companies that purport to contain "tax law changes." They instruct recipients to click on links to download information on topics such as retirement plans and excise taxes.

Instead of providing helpful advice, the links download malware (malicious codes) that can give fraudsters remote access to the target's computer or network. Or they might install keylogger programs that send passwords and other security information to the perpetrators.

Spot the fake

Knowing the signs that an "IRS" phone call or e-mail is fake is the best defense against this type of fraud. For example, the IRS:

- Doesn't use e-mails or phone calls to notify taxpayers, but instead uses the U.S. Postal Service,
- Never needs anyone's mother's maiden name, and
- Doesn't give additional tax refunds.

What's more, the IRS already has taxpayers' dates of birth and Social Security numbers on file. Asking for them is a sure sign that the call or e-mail is fraudulent.

If you or your employees receive phony IRS phone calls or e-mails, forward them to phishing@irs.gov, or report them toll-free at 800-366-4484. Whatever you do, don't click on links or provide any information to callers. Finally, notify your accounting professional. He or she can help you update your fraud prevention program to include these new schemes and instruct employees on how to handle suspicious communications. ■

McGOVERN & GREENE LLP

CPA's & Forensic Accountants

SPECIALISTS IN FRAUD EXAMINATION AND LITIGATION SERVICES

If a business hasn't yet been a victim of fraud, it's been fortunate. According to the Association of Certified Fraud Examiners, fraud costs businesses in the United States billions of dollars every year. Small businesses are especially vulnerable because they often do not have controls in place to reduce the likelihood of fraud.

This is where McGovern & Greene LLP can help. Our firm specializes in helping corporations, attorneys, lenders, law enforcement and governmental agencies analyze financial records and contracts, identify and prevent fraud, recover and analyze evidence, and provide expert testimony in all of these matters. Our highly-experienced team of professionals includes certified fraud examiners and certified public accountants who are experts in the fields of fraud examination, forensic accounting, computer forensics, damage calculations, business valuations and audit services.

Our professionals can assist you in a wide range of matters, including:

- **Fraud Examination**
- **Due Diligence**
- **Training & Seminars**
- **Electronic Discovery**
- **Financial Investigations**
- **Business Valuation**
- **Profit Recovery**
- **Government Contracts**
- **Contract Claims**
- **Forensic Accounting**
- **Asset Recovery**
- **Litigation Services**
- **Economic Damages**
- **Construction Audits**
- **Computer Forensics**
- **Internal Audit Services**
- **Healthcare Audit**
- **Intellectual Property**

CRAIG L. GREENE, CPA, CFE, MCJ

Craig is a leading fraud examiner and white collar criminologist. With over 30 years of experience, he frequently testifies in cases involving financial fraud, accounting, audit, and other disputes involving financial issues. Craig has led many corporate internal investigations focusing on financial statement fraud, corrupt payments, embezzlement and other occupational fraud schemes. He is an international lecturer on forensic accounting and fraud examination issues.

E-mail: craig.greene@mcgoverngreene.com

CONTACT US AT 312.419.1961 OR VISIT www.mcgoverngreene.com
FOR EXPERT FRAUD EXAMINATION AND LITIGATION SERVICES

McGovern & Greene LLP
105 W. Madison Street, Suite 406
Chicago, IL 60602