BERKS BUSINESS 2 BUSINESS
MARCH 2010
Thinking. About Business.

Are You A Target For Employee Fraud?

It's the stage of the business cycle when white-collar crime spikes

By Ted Brubaker and Dave Goss

The Chinese calendar declares that 2010 is the year of the tiger. In Pennsylvania, will 2010 be remembered as the year of white-collar crime?

THE MYTH: *We could never be a victim of fraud.* Despite evidence that employee fraud is increasing at staggering rates, many employers fail to recognize that their organization could become its victim. In reality, every employer is vulnerable to employee theft, especially an organization that refuses to admit this risk exists.

An employer's refusal to acknowledge the risk can come in many forms.

1. Simple denial: *We could never have a problem here.*
2. Misplaced trust: *We have long-term, trustworthy, loyal employees. No one at this business would ever commit fraud.*
3. Misplaced reliance on third parties: *If a threat existed, our accountant would have found it.*

THE REALITY: *Billions of dollars of losses.* According to nationwide studies by the Association of Certified Fraud Examiners (ACFE), U.S. organizations lose 7 percent of their annual revenues to fraud. Applied to the projected 2008 United States Domestic product, this 7 percent figure translates to losses of approximately $994,000,000.

ACFE statistics also suggest that organizations with fewer than 100 employees are the most at risk. These statistics suggest that the median loss suffered by organizations of this size is approximately $200,000. The size of the losses is often directly related to the fact that organizations of this size do not reserve adequate budgets for security services, background checks, or legal services.

In most cases, fraud has led to severe damage to the employer's business reputation, incarceration of formerly key personnel who could not be readily replaced, significant professional fees, and has otherwise harmed the day-to-day operations of the employer's business while attempts at corrective action, including investigations and mitigating adverse publicity, are made. At its worst, as the likelihood of recovering stolen funds is often minimal, employers find that they do not have the resources to withstand any substantial loss. In such cases, employee fraud has led to the downfall of the entire organization, destruction of the owners' equity in the business, and loss of jobs for many innocent employees.

The lingering recession has further increased these threats. Criminal activity appears to be intensifying as some employees are faced with increasing financial problems, which include (1) the employee living beyond his or her means (for example, continued maintenance of a luxury car or mortgage and high credit card debt) and (2) unanticipated financial difficulties (for example, a spouse losing his or her job, significant medical expenses due to a loss of health insurance, or a divorce). Additionally, many employees are dealing with the intensified stress resulting from smaller workforces and contracting revenues. These pressures, when combined with opportunity and personal rationalization by the employee, substantially increase the likelihood of undiresable employee conduct.

THE REACTION: *I can't believe this has happened.* Typically, an employer who has failed to recognize the risk of theft in the workplace is unprepared to address the problem when it occurs. This fact further magnifies the devastating effects on the employer.

THE SOLUTION: *Be proactive but realistic.* It is impossible and unrealistic for an employer to erect invincible barriers that will guarantee the elimination of employee theft. Furthermore, it is not cost-effective to try to implement such internal controls, especially in the case of a small business with limited accounting personnel and resources. The most effective strategies have three components: prevention, detection, mitigation.

1. Prevention. While all fraud cannot be prevented, every employer should adopt policies aimed at deterrence. These policies should be based on a thorough review

and risk assessment identifying the types of fraud that threaten to cause the employer the most economic harm. Common types of fraud include these:

a. Failure to deposit cash receipts
b. Forgery of checks and purchase orders
c. Falsifying timesheets or expense reimbursement requests
d. Billing for services not rendered and collecting the cash
e. Seizing checks payable to vendors
f. Stealing valuable inventory

Of course these types of fraud are not a comprehensive list nor does the list rank the types of fraud with respect to their particular probability or impact. The type, probability, and impact of employee theft will be unique to each employer. However, the goal of each employer will be the same—developing strong controls to deter employees who might otherwise be tempted to commit fraud.

2. Detection. Detection is not intended to prevent but, rather, to uncover fraud when prevention has failed. Unfortunately, fraud can appear in many, but not always obvious, places for employers. These areas include any part of a company in which the employer does not have significant expertise (for example, management of the business's technology systems).

At a minimum, fraud detection requires employers to be vigilant, to follow up on activities that are unusual, to rotate duties, to perform surprise reviews, and to require periodic vacations for any employee who handles payroll or banking duties for the employer. Additionally, detection can be enhanced with anonymous reporting mechanisms (for example, a whistleblower hotline).

3. Mitigation. Mitigation is intended to limit the damage associated with employee fraud.

At a minimum, employers should review and/or consider insurance protecting against fraud. Insurance can be invaluable in covering losses and the cost of an investigation.

Virtual Fraud

By Ted Byrne

"He told me we needed the software package. What'd I know?" the big guy frowned and pointed to his computer monitor. "And I signed the checks for the service … what? For 3 years? So then he said we needed an update that cost more than the initial buy. I asked him, 'Why?'

"And when I realized that every word of his explanation was English, yet I couldn't understand any of it, well.… Look, I started this business. Built it up to almost 200 employees. I'm not so stupid that whole sentences abruptly sound like Serbo-Croatian. So I," he nodded toward the phone, "called my lawyer.

"It was like pulling a thread, y'know? And then the whole sweater unravels? The guy was my IT manager. And the attorney said he'd never heard of the software company. When he checked, it turned out to be a PO box! I was sending checks to a company that my IT administrator owned! For software that apparently never got installed. It probably never even existed. Just bills. Who knew? Who could tell?

"That's when my accountant suggested an IT audit. Turns out IT people are like some kind of druids, speaking a language that no one understands. This guy of mine even had me paying for machines that never came!" He leaned forward now, his fingers tapping on the desktop with each word.

"And we were depreciating that stuff. Tax agents take a really dim view of depreciating equipment you don't own. Or for write-offs on fraudware! I … we … haven't figured out how much we owe yet or what the penalties and interest will come to. It was going on for years. And … and … how much got poured down that rat's hole? These guys say they live in a virtual world. Well it sure sucked in a lot of *real* money from our firm. Worse yet, our bookkeeping and payroll systems all run through our operating system. The accountant's suggesting we do a fraud audit. You know what that costs? On top of the IT audit that's going on?"

This CEO's a composite of a number of regional executives who, faced with recessionary pressures, have begun to look closely at their IT departments. And while most have found ample room for savings and a competent staff anxious to help, business news stories are revealing an increasing few, locally and nationally, who are discovering nasties when they peer into the digital burrows. Many company owners are proud that they could do the jobs of everyone who works for them. Not as well, of course, but they could fill in in a pinch. Everywhere but in IT, where faith has replaced knowledge. And where departments rest upon trust, they have a long way to tumble in a crisis of faith.

"It can cost us tens of thousands at least," the big guy mumbled, bringing his knuckles down. "And right now, in this economy …" he peered up anxiously. "I … I don't know where we'll find that money. Do you?"

Employers should mitigate fraud in a timely and diligent manner in close consultation with experienced counsel. In particular, significant consideration should be given to the individuals participating in any investigation. These individuals should potentially include external auditors, forensic accountants, computer forensic professionals, and legal counsel. The following factors should also be given consideration:

a. Recovery and maintenance of records
b. Notification of law enforcement officials
c. Confidentiality
d. Legal compliance with the gathering of information and interviews of relevant personnel
e. Goals of the investigation

Many employers may be reluctant to involve law enforcement officials as it may increase the length of the investigation and delay the ability of the employer to seek restitution. However, the employer should not overlook the long-term benefits of a zero tolerance policy when it comes to employee fraud.

Finally, the employer should use the mitigation process and experience to reevaluate and reassess the employer's policies and procedures aimed at fraud prevention.

OTHER COSTS: *The indirect costs of fraud.* In addition to the direct financial loss suffered as the result of employee fraud, there are many additional "soft costs" that are often overlooked but can significantly impact the employer's business including these:

a. Possible forced contraction of the business, including possible layoffs
b. Time-consuming distraction to the owners of the business from managing the day-to-day operations
c. Negative effects on banking relationships, which rely on the company's financial statements
d. Loss of the owner's retirement savings
e. Required changes to the internal controls of the employer including changes in business relationships, procedures and forms, and increased internal and external monitoring costs

2010 RESOLUTION: *"Be the tiger.* The effects of employee fraud can be staggering, especially in small businesses and nonprofit organizations, which can least afford the adverse consequences. Strong, effective management includes a proactive and comprehensive approach to preventing, detecting, and mitigating employee fraud. An employer committed to such an approach will be rewarded by significantly reducing the risk of falling prey to employee fraud.

Ted Brubaker, Esquire, (tedb@hublaw.com) is a partner with Hartman Underhill & Brubaker LLP, attorneys at law. He specializes in business law and estate planning. Dave Goss, CPA/CFF, CIA, CFE, (david.goss@parentebeard.com) is a partner with ParenteBeard LLC. He specializes in fraud and forensic/litigation services.