

Fight Internal Fraud

Internal controls and policies help deter fraudsters

By Joel Bartow

When people hear the term “internal fraud,” the name Kenneth Lay may come to mind. While the Enron scandal certainly made headlines, you might be surprised to know that this type of fraud—financial statement fraud—only accounts for 8 percent of all fraud. It is the other 92 percent of fraud that people should, in fact, be concerned with.

Today, occupational fraud is at an all-time high and the cost is staggering. The typical U.S. organization loses 6% of annual revenues to fraud, according to the Association of Certified Fraud Examiners (ACFE), a membership organization in Austin, Texas. That’s some \$660 billion in total yearly losses throughout the U.S. ACFE’s figure is just an estimate because many firms don’t report frauds, those that do can’t always determine the actual costs of such crimes, and many corporate scams go unnoticed.

The risks to businesses from corporate swindles are greater than ever. Though organizational complexity is increasing, companies historically pay little attention to fraud, under-staff internal audit functions, and accept some fraudulent activity as “the cost of doing business,” according to London, England-based consultancy Ernst & Young Ltd.

The proper procedures and tools, however, can help prevent many workplace crimes. But make no mistake: Businesses unable or unwilling to identify and control such problems do so at their own risk.

Pinpoint Fraud

The first step toward eradicating fraud is to identify your greatest risk factors. Top offenders commonly include the failure to split key duties among several employees; inefficient physical and procedural safeguards over cash, other assets, and transactions; inadequate supervision of employees; and lack of mandatory vacations for employees with financial responsibilities.

The hard part is to recognize actual fraud. ACFE classifies primary corporate scams as asset misappropriation, corruption, and fraudulent statements. While employees pilfering cash or company resources such as equipment, inventory, or information represents the most conventional fraudulent behavior, corrupt employees engage in far more costly occupational schemes such as bribery and kickbacks. Indeed, the most prevalent form of corruption involves purchasing agents rigging contracts for favored vendors. With employees receiving payoffs and delivering payola covertly, such corrupt practices often escape detection until and unless other employees or vendors blow the whistle.

Of course, simply recognizing and reacting to fraud is insufficient. You must eliminate what the late sociologist Donald Cressey called the “fraud triangle,” which involves a potential scammer’s immediate financial needs, opportunity to meet those needs, and ability to rationalize the crime.

To deter such activities, establish fraud-prevention guidelines, ethics codes, and internal controls. Background checks on low- and high-level recruits can weed out possible criminals, while tip hotlines encourage employees to police themselves and co-workers. Requiring workers to take time off and separating financial responsibilities can eliminate temptation, while promising crooks you’ll terminate, prosecute, and otherwise discipline them makes it clear you tolerate no fraud.

Background Checks

Conducting background and credit checks on employees who would have access to credit card and other financial data is a no-brainer, but determining if someone has a criminal record is no easy task. Private-sector organizations, for example, have no access to the FBI’s National Crime Information Center. You can, however, ascertain potential staffers’ backgrounds by using their social security numbers and residential addresses to establish past criminal histories in those specific locales.

Credit histories can turn up financial problems, such as delinquent bill payments and gambling habits, which can drive employees to crime. After all, people who don’t pay bills can rationalize other deceptions as well. Be sure to place workers with money problems in positions with no financially related responsibilities.

Dig deeper into the backgrounds of employees seeking senior positions. In addition to performing extensive online publication searches, debt analyses can indicate the extent of a potential executive’s delinquency, a situation that can exert significant financial pressure. Some high-level administrators, for example, live above their means by driving expensive cars, sending children to private schools they can’t afford, or accruing huge credit card debt. You would be wise not to hire such persons for financially sensitive positions.

Internal Policies and Procedures

Ethics policies should clearly detail what you consider to be illegal, improper, and fraudulent behavior. New employees should receive and sign statements that delineate what they can and can’t do.

Your best policies and procedures won’t work, however, if employees don’t know about them, or they have no teeth. Enron, after all, had a code of conduct, as ACFE points out. Educate existing and new employees – including executives -- about the use of such policies and the penalties for defying them, and update such training yearly.

Specific crimes require specific solutions. To prevent check fraud -- which costs U.S. companies more than \$10 billion annually, according to the National Check Fraud Center in Charleston, S.C. -- implement Positive Pay. The process guarantees that banks honor only those checks that match exactly the checks that appear on a list you provide them.

Foil credit card fraud by limiting employee access to customers' credit card numbers. As soon as a customer enters an order, change the first 12 digits of the credit card number to Xs to prohibit employee access.

Recent technological advances can prevent some Internet credit card fraud. The address verification system (AVS) protects against random credit card generation and bogus billing addresses by verifying that the latter is the credit card holder's actual address. Should the wrong address get through, the additional security layer of a card security value (CSV) would catch the fraud. By the end of 2004, all credit cards must have the three-digit CSVs.

Thwart employees from fraudulently diverting shipped items to themselves by cross-referencing all shipping addresses with employee residences. Check the system regularly to ensure merchandise gets to the correct locations. Deter procurement fraud by creating an approved vendor list that ensures you pay only vendors that pass background checks.

Separate Duties

It's critical to separate financial tasks among several employees. The person who signs checks, for example, should not make bank deposits. Budgetary cutbacks and downsizing, however, often result in the same person handling multiple procedures such as taking orders, readying invoices, and documenting transactions.

Further compounding such an invitation to fraud is when those same employees -- fearing that other employees might discover their nefarious deeds -- work unusually late and on weekends. Workers who are never sick, take no time off, arrive early, and stay late may be hiding criminal activity. Requiring all employees to take vacations often uncovers fraud that your "best employees" perpetrate. It's difficult to keep a house of cards from tumbling during a mandatory holiday -- especially if another employee performs the vacationing worker's tasks.

Blow The Whistle

Because whistle-blowers expose a large percentage of frauds, 24-hour tip lines encourage employees to report potential offenses that security professionals can investigate. Publicize the confidentiality and anonymity of fraud-prevention hotlines, which are most effective and secure when outside subscription services run them. Keeping employees abreast of such reporting mechanisms demonstrates your intolerance for fraud and limits would-be corporate villains' opportunities.

You can't eradicate corporate fraud completely. You can, however, minimize its damage and take appropriate actions to prevent it. Whether you choose to publicize fraud in your company or not, make it clear that you will find and fire fraudsters. If necessary, let your employees know you will drag criminals out of the workplace in handcuffs and prosecute them to fullest extent of the law. The competitive reality is stark but simple: Create an environment where fraud can't thrive and you'll survive; if you don't, you will soon be out of business.

Joel Bartow, CFE, CPP, CBM, LPI, MA, is Director of Fraud Prevention with ClientLogic in Nashville, Tenn. A Special Agent with the FBI for 10 years and a licensed private investigator for seven, Mr. Bartow investigated international money laundering and Russian organized crime. He is an Associate Member of the Association of Certified Fraud Examiners, a member of the American Society of Industrial Security, a Certified Fraud Consultant with the International Fraud Training Institute, and a member of the International Association of Chiefs of Police.

#####