Mountain Plains Journal of Business and Technology

Volume 8 | Issue 1 Article 2

Date Published 10-1-2007

The Enemy Within: A Commentary on The Exploding Problem Of Employee Theft

Kenneth W. Hollman
Middle Tennessee State University

Robert D. Hayes
Tennessee State University

James R. Mahurin
Society of Risk Management Consultant

THE ENEMY WITHIN: A COMMENTARY ON THE EXPLODING PROBLEM OF EMPLOYEE THEFT

KENNETH W. HOLLMAN
MIDDLE TENNESSEE STATE UNIVERSITY

ROBERT D. HAYES
TENNESSEE STATE UNIVERSITY

JAMES R. MAHURIN
RISK MANAGEMENT & INSURANCE CONSULTING

ABSTRACT

Few companies recognize the big bite that thefts, both large and small, take out of their profit margin. It is estimated that theft in some form absorbs 5 percent of all business revenues, which translates into about $652 billion in losses per year. Small businesses take a disproportionate share of the hit. The purpose of this paper is to highlight the rapidly expanding scope of the employee theft problem and to suggest common sense Risk Management techniques that companies can use to prevent losses and to reduce the damages from those that occur. In many cases, the loss control measures are inexpensive and easy to implement.

I. INTRODUCTION

There is widespread agreement that occupational fraud and abuse is big business, that it is widespread, and that it is beginning to reach epidemic proportions (Coffin, p.8). Firms of every size in all industrial categories and at all organizational levels are victims of fraud and abuse by their own employees. Occupational fraud—whether asset misappropriation, corruption, or fraudulent statements—is one of the costliest problems facing business today, particularly small private firms (Anonymous 1, p. 11), and despite massive efforts to contain it, it is one of the fastest growing industries in the country. Thefts of company assets more than doubled from 1999 to 2004 (Anonymous 2, p. 56) as the employee theft problem began to spin out of control. Occupational fraud affects, or has the potential to affect, every business in the country (ACFE, p. 8). Risk management of theft and other crime exposures is extremely important, and no employer should be naive concerning the magnitude of the problem or blissfully think or hope that it will never happen to them.

The purpose of this paper is to heighten employers' sensitivity to the employee dishonesty problem and to help them better understand and control employee theft. The paper emphasizes how critical it is for them to learn as much as possible about

occupational fraud and the devastating financial impact that it can have on a firm's bottom line or even its solvency. Perhaps even worse, insider theft can insidiously corrode trust and confidence between employer and worker—the glue that holds the workplace together. It saps employee morale and diverts the attention of managers from other tasks.

To achieve its purpose, the remainder of the paper is divided into seven sections. The first explains the scope of the employee crime problem, and the second offers lessons and insights into who commits occupational fraud. The third section discusses the elements that must simultaneously be present for fraud to exist, and the fourth section discusses reasons why more thefts are not reported. The fifth section provides some commonsense observations about how the impact of theft can be prevented or reduced—what companies can do to help deter fraudulent conduct. The sixth section explains how the risk of financial loss by theft can be transferred to an insurance company, and the final section contains the summary and conclusion of the study.

II. SCOPE OF THE PROBLEM

Statistics on employee theft are astounding. U.S. companies lose more to internal fraud than to shoplifting, although shoplifting incidents tend to get more press (Ryan, p. 8). According to one source, employee theft and fraud accounts for 30-50 percent of all company failures (Lurz, p. 112), and in the retail field, theft accounts for 80 percent of all losses (Ritter, p. 25). These findings have serious implications for small businesses that face increasing margin pressure from all directions. It means that billions of dollars of profits hemorrhage away each year and that the premiums they pay for commercial insurance are driven up. It also means that consumers end up paying higher prices for the goods and services they purchase.

Statistics on employee dishonesty gathered by the Association of Certified Fraud Examiners (ACFE) show that firms lose on average $9 per day per employee for insider theft (Lurz, p. 112). The median dollar loss came to $159,000, which amounts to about 5 percent of all annual revenue, and for all businesses, the tab comes to about $652 billion per year (ACFE, p. 8), making fraud an industry of its own (Coenen, p. 1). Another source, using a different methodology, suggests that the problem is more rampant than the ACFE figures indicate. It reports that employee theft costs businesses an astounding 20 percent of every dollar earned (Gips, p. 16). The repercussions of employee theft are far more harmful to the bottom line than has traditionally been recognized, and the impact is more far-reaching. Three in five privately held companies can expect to be victimized by employee-perpetrated theft of funds or equipment in any given year (Anonymous 1, p. 11).

III. WHO ARE THE "ACTORS"?

Trusted employees from all walks of life, from all income ranges, and in every business discover creative ways to make their job more rewarding. Every employee is a potential suspect when it comes to who is capable of committing fraud, i.e., from a low-level staff member to a highly educated, hard working, seemingly mature and responsible senior officer. Some observers say that 6-8 percent of all employees have taken or have considered taking money from their employer (Knapshaefer, p. 45). There are more ways for an insider to take advantage of their workplace than most executives can imagine. Too often, companies set themselves up to be victimized by theft. The opportunity for employees to divert company funds into their own pockets is simply handed to them because of weak internal controls and oversight (Cressey, p. 30).

The level of authority a person holds within the organization tends to have a significant impact on the size of loss in a fraud scheme. Most insider thieves are not aloof loners, introverted nerds, or high school dropouts. Rather, the typical perpetrator is a married, college-educated white male who exhibits all the qualities one looks for in an employee—high integrity, trustworthiness, and devotion to the job—and who is higher up the organizational ladder (Tyska, p. 17). While there may be more stings by rank-and-file employees (41.2 percent) simply because of their greater numbers, the take per person is much larger at the higher levels. On average, losses from fraud by owners and executives are nearly five times larger than those of managers and 13 times higher than those caused by employees (ACFE, p. 5). Senior members and owners of an organization are more likely to be in positions of trust, to have access to the money and books, and to have authority to override or change control procedures in order to conceal the fraud (ACFE, p. 42).

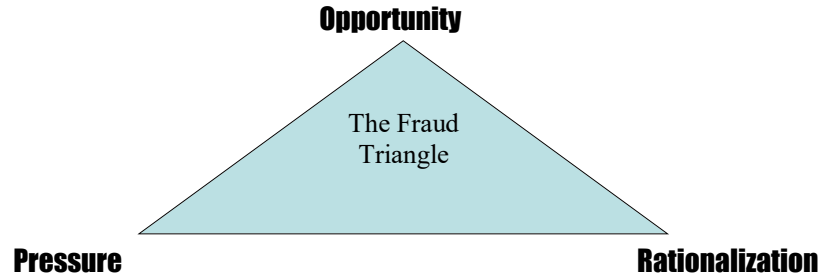
Men commit 61 percent of all insider crime offenses, and the median loss caused by men is two and one-half times greater than those caused by women, $250,000 to $102,000, respectively. At least a part of this disparity is a result of men tending to hold more management and executive-level positions in many organizations. As the perpetrator's age rises, so do the losses from their fraud. The median loss for those age 60 and over is 28 times greater than that for those 25 or younger. There is also a strong correlation between the education level of the perpetrator and the size of the median loss. The median loss caused by those with postgraduate degrees is over four times greater than losses caused by those with high school diplomas (ACFE, pp. 44-45).

The costliest theft cases occur in organizations with fewer than 100 employees. One important reason why small companies bear the brunt is that small companies cannot afford the kinds of sophisticated internal controls and systems that prevent or deter embezzlement. Schemes at small businesses cost an average of $190,000, higher than the median loss in even the largest organizations (ACFE, p. 5), and help contribute to the short lifespan of such businesses (Mohsin, p. 271).

It is interesting to note the effect of computers on the average size of insider thefts. Technology has dramatically increased the size of insider theft jobs. The average employee embezzlement comes to $25,000, but higher dollar volumes are associated with computer-assisted thefts, which average $430,000. When coupled with poor controls, computer embezzlement can be very difficult to detect, especially when it involves sophisticated measures, collusion, and the falsification of documents (Knapshaefer, p. 44, and Lurz, p. 112). The massive infusion of computer technology into the workplace has clearly raised the bar for the minimum level of loss control protection most companies need.

IV. THE FRAUD MODEL

Understanding the elements that precipitate employee fraud is the first step in a program to prevent it. Criminologist Donald R. Cressey interviewed nearly 200 incarcerated embezzlers in the late 1940s and developed a fraud model, which has become known as the "Fraud Triangle," containing three factors that are necessary and sufficient conditions for fraud to result. The three factors are perceived pressure facing the perpetrator, perceived opportunity to commit and conceal the crime, and the person's attitude or rationalization of the fraudulent act. While later researchers have refined the Cressey model, it remains much as he presented it almost 60 years ago. The Fraud Triangle is depicted below, and the three key variables that must be present simultaneously for a fraud to occur are discussed in the following sections.



Source: Adapted from Auditing Standards Board (ASB), Statement on Auditing Standards No. 99, Consideration of Fraud in a Financial Statement Audit, New York: AICPA. Issued October 2002.

V. MOTIVES/PRESSURES TO STEAL

Motives for stealing rest on unquantifiable human instincts and are as highly subjective, messy, and diverse as the nature of human character. The three major reasons are lifestyle, finances, and emotions. The lifestyle factor becomes operative when workers steal money to pay off an out-of-control credit card debt (McCormick, p. 122) or to enhance their lifestyle with the purchase of a bigger house, faster car, expensive recreational property, or extravagant vacation (Wells, p. 1). They take advantage of an opportunity to steal because of weak or unenforced control policies and procedures. They may rationalize that everyone else is doing it.

The financial factor comes into play when the worker needs more money to meet medical costs or to defray other emergency expenses. The worker may see the employer as a faceless and avaricious giant with a corrupt ideology who will never notice the loss of a few dollars, a few pieces of apparel, a few supplies, or a little bit of merchandise (Ritter, p. 25). Some workers may steal for the thrill of it, or they may appreciate and need the challenge of stealing—using their sophisticated understanding of the firm's technology or its financial statements to mastermind an elaborate scheme (Knapshaefer, p. 43).

The emotional factor becomes operative when an inequity-sensitive worker feels that he/she is not being treated well. He/she may have missed a promotion or feel underpaid, or feel an unfairness in pay, perhaps because a proximal referent in a similar position in the same or a different company is earning a higher salary and/or working fewer hours (Fishman, p. 61). Feeling overworked and/or underpaid, he/she seeks revenge in the most convenient way possible.

VI. OPPORTUNITY TO STEAL

A simplistic answer as to why employees steal is to say that they are in a position to take what does not belong to them and that it is easy. After all, employees have full access to the crime scene (Ryan, p. 8). They know the firm's procedures and policies, cultural norms, and networked information systems, and they will likely know their fellow workers and their habits. In many types of business, i.e., convenience stores, employees work with only one or two other employees and may be left alone on a routine basis. They have ready access to the cash register and to concealed places where high-ticket items are kept, thus optimizing the opportunity to steal. In such idyllic circumstances, some workers cannot resist the temptation to take advantage of and exploit any weaknesses or vulnerabilities they see in management controls.

Distilled to its basics, the primary reason employees steal is that employers create the environment for it. They steal by design and exploit opportunity simply

because they can, i.e., the employee is in a position to override all internal accounting or financial procedures. There is ineffective oversight (Ritter, p. 25). The failure to consistently enforce and constantly monitor management policy, procedures, and accounting controls and to create an ethical environment that discourages dishonesty will inevitably lead to a loss of assets that can devastate the company's profit margin.

1. EMPLOYEE RATIONALIZATION

In most cases, employee theft begins innocently enough (Ritter, p. 25). For example, the thief might be an executive who has extensive knowledge of how the company operates, learns how to ignore or circumvent established controls, and is the beneficiary of a system that functions on the assumption that he is trustworthy. He may lose his moral compass and "dust the cash register" to supplement his salary for $10,000 cash to capitalize on a business opportunity for which funding is not otherwise available. Or he may be dealing with a personal issue such as a gambling or drinking addiction or even a mental problem that leads him to a life of crime. He may view the transgression not as stealing but simply as borrowing funds that will be repaid when his financial situation improves or when he achieves the success that has heretofore eluded him. He thinks the company is too big to notice. He is probably firmly convinced that he is smart enough to conceal his duplicity, and he usually does for a while. The median length from the time the scheme begins until it is detected is 18 months (ACFE, p. 4).

Alternatively, the culprit might be a single-parent mother in a low-level position who finds herself late on credit card payments or needs to purchase a big-ticket item. So, she may pilfer company supplies or "short" the cash drawer for a "little" cash to help meet the down payment on a much-needed new car. She has every intention of returning the money next month but then "forgets" to do so. After a period of time during which her initial attempt goes without detection, she "borrows" money again, perhaps in a slightly larger amount, and the abuse escalates into ever more frequent and more serious events. And the pattern continues, with the thief becoming more anesthetized to the wrongdoing and ever more confident that she can hide any traces of her theft. She inflicts ever more serious financial damage as the incidents pile up.

VII. WHY MORE EMPLOYERS DON'T PROSECUTE

Employers often place great trust and have implicit faith in their employees. They may think of them as extended family that are honest, hard-working, and have only the company's best interests at heart. Sometimes employers refuse to believe that they are a victim of theft, particularly if the theft is by a long-term, trusted, and

heretofore presumably loyal employee, right up to the moment that incontrovertible evidence forces them to confront the awful truth.

The victimized employer is first likely to be astonished, shocked, and angry, to feel hurt, and to experience an utter sense of betrayal. Then follows the dread of reputation degradation—the fear that public knowledge of employee theft and dishonesty in the organization will endanger the trust of customers and negatively impact sales and revenue, since dishonesty or deviant behavior in one department may be perceived by observers to be the underlying behavior across other departments (Anonymous 2, p. 56). This helps to explain why the latest ACFE study shows that the victim organization referred the case to a law enforcement authority only 70 percent of the time (ACFE, p. 56). Other sources report a much lower referral rate. One study indicated that only 40 percent of employees caught stealing are referred to the criminal justice system and only 20 percent are required to make some form of restitution. Almost unbelievably, the remaining 40 percent face no civil or criminal penalty (Lurz, p. 112).

Hence, many employers choose not to prosecute the employees who prey upon them. They would rather handle problems of occupational fraud quietly and without police involvement (Coffin, p. 8) by discreetly firing the perpetrator and refusing to serve as a reference in the future (Lurz, p. 112). The alternative is to face the specter of negative publicity, embarrassment of having unwittingly fallen prey to an inside con artist, public humiliation of the company, difficulty in getting future loans, and enormous time obligations and costs (legal and investigative fees) of prosecuting the guilty employee. And there is no assurance of full recovery, or any recovery, even with a favorable verdict. Only 20 percent of all fraud losses are ever recovered, including proceeds from restitution and insurance, and 37 percent of victim companies never recover any funds at all (Coenen, p. 1).

Admittedly, employers face a dilemma with regard to monitoring their employees. They wish to trust their employees, have faith in their integrity, and create an environment of mutual confidence and respect between management and workers. However, as stewards of the firm's and possibly their own assets, managers have the fiduciary responsibility to safeguard and protect those assets. Hence, some managers have opted to use surreptitious devices such as hidden cameras to detect employee theft. This practice may go against the grain of many small firms that attempt to create an environment where employees are trusted. Some small firms may feel that degradation of the work environment can lead to an adversarial worker–employer relationship, diminished productivity, and other dysfunctions. The key is to strike a balance between placing confidence in persons once they are hired and

creating strong internal controls at a reasonable cost to eliminate their temptation to steal or to commit other fraudulent acts (Knapshaefer, p. 45).

VIII. PREVENTION

A priori evidence indicates that the most cost-effective way to deal with fraud is to prevent it. Hence, companies should exert every effort to prevent exploitation via insider theft and fraud, though they will probably never be so clever as to design a foolproof system to thwart all human shortcomings (Fishman, p. 60). The most prudent measures are to screen employees for characteristics associated with low-theft activity before hiring them and to take preventive steps after the hire by establishing and implementing sound internal controls—checks and balances that help to prevent fraud and to limit financial losses when fraud occurs. The company should review these management control policies periodically and update them as needed. As an example, when Internet channels are added, the company should make sure that this does not open new avenues for potential fraud (Knapshaefer, p. 44).

To deter abuse and thefts, companies should look for areas of vulnerability. Identifying the areas of operation most affected by theft enables top management to measure the effectiveness of loss prevention and reduction programs, to focus on problem areas that have the greatest potential for improvement, and to formulate strategies for preventing fraudulent schemes (Anonymous 1, p. 11). While there are no simple, foolproof solutions to the prevention of fraud, here is a list of positive, structured loss-control initiatives gleaned from the literature, none of which require a huge investment in infrastructure or personnel that companies can use to avoid or mitigate the effects of theft and fraud.

1. DUAL CONTROLS

Separation of employee duties is a strategy that can help the internal control system to work. Firms make themselves vulnerable to theft and fraud if they do not develop and implement policies about how financial transactions are initiated, authorized, recorded, and reviewed. Since 30 percent of all occupational fraud is committed by employees in the accounting department (ACFE, p. 5), it is essential that different employees should handle different accounting and financial tasks. Those who make decisions about what equipment, materials, and supplies will be purchased or what work will be performed should be separate from those who handle the checkbook or are in charge of payments to suppliers or vendors. A scenario in which ordering and payment are the responsibilities of just one person is fraught with the danger of fraudulent expense reimbursements in the form of skimming (accepting payment from a customer but not recording the sale), cash larceny (taking cash or checks from daily receipts, which have been recorded, before they can be deposited in

the bank), kickbacks, or other forms of occupational fraud. When duties are segregated, each area can act as a check against abuses by the others (Lurz, p. 112).

In particular, to maintain adequate cross-departmental responsibility, the controller (with accounts-payable duties) should not supervise purchasing and receiving. Rather, in order to minimize the opportunity for fraudulent billing practices, the controller, purchasing agent, and receiving agent should report separately to senior management. It is far better for the purchasing department to negotiate the contracts for equipment or work, an operations unit such as receiving to verify that the equipment is delivered or the work is done according to specifications, the accounting department to process the purchase order, and senior management to sign the check. Owners should check all orders to make sure they are accurate and of the quality intended. A firm set of dual checks and balances (a control technique called redundancy), with multiple executives signing off on trade contracts, funds allocations, and disbursements, is a key way to prevent temptation and to help stem the rising tide of employee theft and abuse. Subsequent bookkeeping adjustments, even minor ones or adjustments made to correct an error, should be approved by the owner or a trusted assistant (Mather, p. 8). Of course, even the most elaborate control system can be circumvented if two or more people collude to commit the fraud (Lurz, p. 112, and Fishman, p. 60).

Dual controls with separate decision making, authorization, and paying functions are more important in smaller firms than larger ones. The reason is that multiple responsibilities (i.e., asset custody and accounting responsibility) often fall upon the shoulders of a single employee in a small firm. That person could easily have both the opportunity and means to conceal theft. It is difficult to design foolproof systems in such circumstances that eliminate the ability to conceal theft if the employee is savvy enough to know the loopholes in the system and to hide those loopholes (Knapshaefer, p. 45, and Lurz, p. 112).

A small business is particularly vulnerable if only one person is involved with or looks at a single transaction—that is, the same person is responsible for decision making (buying), authorizing payment, and writing the check. Any person empowered to both record and process a transaction is in a position to engage in check tampering—to either steal and then forge a check, issue a genuine check to a fictitious entity, alter a legitimately issued check, duplicate (print) a counterfeit check, or engage in some other check fraud scheme. The challenge to the management of a small business is to find the appropriate level of staffing and to designate the appropriate persons to have supervisory authority, without giving authority to many people and spending inappropriate amounts for loss prevention activities (Knapshaefer, p. 45).

2. HIRING GOOD PEOPLE

The fight against theft starts with the pre-employment screening procedure for new hires that will have access to organizational assets. The employer should use selection and detection procedures such as conducting reference checks and running background verification and searches to find out as much as possible about the applicant's previous experience with other employers and law enforcement authorities. This information can be obtained for modest sums, in some cases as little as $10 per employee (Mather, p. 8).

Depending on the position, screening may include drug tests, credit histories, honesty (integrity) tests, and driver's license and criminal records checks on all applicants, particularly those who are in sensitive positions that involve the flow of money or have access to checks, credit card numbers, or other items that are easily stolen. Screening can uncover job applicants who lie on or embellish their resumes or fail to include crucial information regarding criminal convictions and thus present a significantly higher risk for potential problems. Pre-employment screening, because it reduces the company's vulnerability to the risk of theft, is an extremely important anti-fraud technique since prevention is more cost effective in the long run than prosecuting the employee and attempting to recover losses (Wells, p. 1). It is best for employers to hire workers with a high level of cognitive moral development and then to treat them as trustworthy and honest once they are hired (Appelbaum et. al., p. 175).

It is worth repeating that the company should put emphasis on hiring only the most qualified and trustworthy employees. Managers should be educated about how to use interview techniques that help distinguish honest from dishonest applicants. For example, it is better to ask open-ended questions during the interview process. Open-ended questions tend to be more revelatory about the candidate's background, attitudes, and behavior patterns (Ritter, p. 25). Also, there should be multiple interviews and interviewers for each applicant (Ryan, p. 8). Taking sufficient time to properly interview potential employees is an investment that will reap huge dividends down the road, enabling the employer to ferret out the predatory employee who seeks employment with the goal of defrauding the employer (ACFE, p. 55).

Interviewers should review resumes for evidence of job hunting and avoid putting those with a multi-job history in payroll administration, accounts payable, or other key financial positions. The interviewer should also discuss issues of ethics and ask the candidates to discuss any ethical dilemmas they have experienced in the past (Lurz, p. 112).

3. ETHICS MANUAL

Employees are opportunistic about stealing on the job (Lurz, p. 112). They are more likely to engage in occupational fraud and abuse if they know the company is not taking an aggressive position regarding employee theft and, after weighing the risks, believe there is a fairly good chance they will not be caught. It is well established that the lower the risk of being caught stealing, the more likely it is that a theft will take place. Fraud seeks the organization with the lowest level of protection (Knapshaefer, p. 43).

The ethical culture of an organization can only rise as high as the standard set by top management. Members of the management team have an important role as authority figures and, as such, have the duty to initiate and implement a corporate culture that focuses on and reinforces honesty (Appelbaum et. al., p. 175). All fraud starts with the owner (Dennis, p. 55), and management that is perceived to be unfair and dishonest will beget dishonest employees (Wells, p. 1). Hence, there is a need for a written guidebook or manual containing the organization's code of conduct and ethics policies that emanates from and has the firm support of the senior management of the corporation, whose ethical conduct serves as a benchmark for the organization's employees. The manual should be made available to every manager and to every employee in every department.

The manual should clearly define behavior expectations, i.e., what activities are unacceptable, the internal controls in place to prevent fraud, and the punishment for those who do not comply. The ethics policy should become operative at the time of new hire orientation and continue until the employee separates. Workers exposed to a work group that condones theft will be more likely to steal (McClurg and Butler, p. 25). Hence, companies should imbue workers at the time of hire with the notion that preventing fraud is an all-hands responsibility and that every worker is accountable for his/her own actions and should share responsibility for the values and beliefs of the organization.

After the hire, the firm should sponsor positive and non-accusatory loss prevention awareness classes, workshops, and refresher briefings and provide other broad-based education updates and reinforcement of the ethics policy on an annual basis. Each employee should be required to sign off on the policy every year. There should be strong and consistent signals from the organization that any form of theft is unacceptable. The point should be driven home that ethics are not just a moral imperative, but the foundation of good business and that employee dishonesty eventually costs everyone in the company through higher prices and thus lower profits, adverse publicity, and decreased morale (Wells, p. 1). If the ethics policies and

the emphasis on integrity are in a manual, are strictly implemented and regularly evaluated (Mohsin, p. 271), and are repeatedly mentioned in intra-company training sessions and the sanctions for ethical shortfalls are spelled out and are vigorously enforced, a climate is created and fostered whereby employees remain focused on ethical behavior.

The ethics manual should be used in conjunction with well-defined accounting procedures and written job descriptions to establish accountability for each staff member. When lines of authority and responsibility are clearly delineated, it makes it much easier to hold people accountable, to monitor their performance, and to encourage them to act with integrity in the conduct of company business (Lurz, p. 112, and Mohsin, p. 271). Of course, even the clearest lines of responsibility and authority can be abused by a dominant manager who chooses to override or circumvent the system to commit fraud.

IX. OTHER PREVENTIVE MEASURES

Companies can use many other accounting policies and financial and organizational control features to flag and combat potential fraud, limit or mitigate the amount of damage that can be done, and provide optimum protection for the business, including:

a) Accounting Policies

- Implement and strictly enforce a rule that no one in the purchasing area can take bribes (such as inflating invoices from a vendor and in return receiving 10 percent of the invoice price as a kickback), or accept gratuities (say from a vendor as a token of the vendor's appreciation for their help). Nothing should be accepted—no entertainment, no free vacation, no beverages at Christmas, nothing. Without such controls in place, purchasing agents may be tempted to accept kickbacks (Lurz, p. 112).
- Use an independent party who is not involved with the daily checkbook transactions (collections and disbursements) to reconcile monthly bank statements before they are passed to the bookkeeper, and rotate both functions every few months (Mohsin, p. 271).
- Document and scrutinize all reimbursable expenses incurred by employees. It is easier to detect and trace fraudulent transactions and avoid paying phantom or padded travel and nonexistent meal costs if specific documentation is required for reimbursement and if every employee expense voucher is subjected to a pre-audit review before it is paid (Mather, p. 8).

- Restrict access to assets of physical value, such as inventory, to authorized employees, particularly if the assets are readily marketable and easily manipulated like jewelry or computer chips (Meiners, p. 53). Conduct inventory audits on a periodic and sometimes unannounced basis to uncover pilferage or other misappropriation of non cash assets. Random audits increase (1) the thief's risk of being caught before he/she has the opportunity to alter, destroy, or misplace records or other evidence (Wells, p. 1) as well as (2) the company's chances to uncover under-the-table dealings (Tyska, p. 18). Studies reveal that companies with internal audit departments that regularly perform surprise audits suffer median losses about one-half the size of those that do not (ACFE, p. 4). Audits help identify new vulnerabilities, measure the effectiveness of existing controls, and serve as a guide in the design and implementation of a better control system. It is also prudent to use a third party to reconcile sales to inventory on a periodic basis.

b) Financial Control Features

- Since the asset that fraudsters target most often is cash, including checks and money orders (ACFE, p. 12), it is prudent to keep cash and other highly liquid assets in a well-secured location. As a further measure to discourage theft attempts, companies can mine transaction data such as checking accounts, purchase orders, sales receipts, and other key documents to detect fraud of these items with good internal audits. It is a good idea to conduct an external audit on a periodic basis to assess the control performance of the firm and provide an independent evaluation of current internal audit practices (Mohsin, p. 271).
- Institute a rule that all company credit cards must be signed out and all credit card expenses authorized by a purchase order (Mather, p. 8).
- Checks should be signed only after carefully reviewing the supporting documentation (invoice, delivery receipt, purchase order), and then only the owner or a trusted assistant should have the authority to sign checks. Audit the check-issuing process, keep blank checks under lock and key, and make sure checks are printed using the latest counterfeiting technology (Mather, p. 8).
- Show attention to and embrace responsibility for the financial health of the organization. Ostentatious displays of excess and disregard or indifference by managers toward their role and responsibilities is an invitation for employees to take advantage of their laxity and complacency. A haphazard and cavalier attitude toward rules and regulations by management will filter down to and will soon be reflected in the attitudes of employees (Coenen, p. 1).

- Maintain an ongoing process that facilitates measurement of the impact of loss control programs. Regularly review and evaluate procedures that are implemented (Mohsin, p. 271).

c) Organizational Control Features

- Take responsibility as owner for approving all vendors and counting all goods received or delegate such authority only to a trusted assistant. This will prevent conflict-of-interest situations from arising, such as an employee owning an undisclosed interest in a supplier and then negotiating a deal with the supplier, perhaps purchasing materials at an inflated price (ACFE, p. 17).
- Refunds are a huge cost center in many kinds of business. Institute a third-party refund policy whereby refunds are issued only with the approval of the owner or a trusted assistant (Mather, p. 8).
- Make sure that each employee takes vacation time. This gives others the opportunity to see the books when an employee is away and to expose any schemes in which he/she might be engaged. Periodic job rotation is suggested for employees in sensitive positions in order to reduce the opportunity for fraud (Mohsin, p. 271).
- Encourage open communication between management and staff. Let everyone know the company is seeking information concerning larcenous intent and designate two "bypass" people or "go to" people (male and female) whom employees can approach confidentially about any suspected theft or fraud within the organization (Coffin, p. 8). The company can simultaneously create a "watch-dog" (incentive) program for associates who uncover misconduct.
- Many workers feel outrage when they know there is a thief among them. A company can cash in on the moral fiber and goodwill of its employees by establishing a fraud hotline for employees (or customers or vendors) to anonymously report suspicious, unethical, or illegal activity to management, with no fear of job loss or other recriminations (Ryan, p. 8). The reporting medium may be an anonymous phone call, a confidential hotline managed by a third party, an anonymous letter, or an anonymous message in a designated area of a website (Wells, p. 1). Occupational fraud, particularly if it involves a large amount of money, is far more likely to be detected through a tip than by other means such as internal audits, external audits, or internal controls. The ACFE has found that 34.2 percent of all fraud schemes are uncovered through tips (ACFE, p. 28). Getting workers involved in the discovery of unethical and dishonest conduct is a key element in creating a culture based on honesty.
- Theft is unacceptable. It is a crime, and those who commit it should be treated as criminals (Schroeder, p. 86). The rapport between management and employees is reinforced if a zero-tolerance policy is instituted whereby every

wrongdoer is prosecuted to the fullest extent of the law for every infraction, large or small, even in the face of police and prosecutorial resistance (Longmore-Etheridge, p. 74). An immediate and consistent response to theft, even though it is unsettling to trace through years of historical financial data and the results may be only marginally productive, sends a signal to the staff and makes public the fact that those who steal do not do so with impunity and that the firm is serious about curbing insider fraud.

X. NEED FOR INSURANCE

Every company should have Commercial Crime Insurance (CCI) to cover employee dishonesty and theft. This policy covers most forms of occupational fraud, depending on the type of perils coverage the insured chooses. Despite its obvious importance, however, it is vastly undersold. One study showed that less than one-fourth of all businesses purchase crime insurance (Anonymous 1, p.11), and other studies have shown that too often firms that have it do not have sufficient limits (McCormick, p. 122).

CCI policies are designed to indemnify the employer against employees who commit fraud for their own personal benefit or cause the insured to sustain a loss. Theft in the form of robbery, burglary, embezzlement, commercial bribery, or stock fraud is covered. The burden of proof is on the insured to prove that a loss occurred. Unexplained inventory losses are not covered. As might be expected, the policies contain subrogation provisions permitting the carrier to sue the wrongdoer up to the amount of indemnity (Wells, p. 1).

The most recent crime insurance policies require the insured to give notice of loss to the carrier as soon after discovery of loss as possible and to provide proof of loss, if requested, within 120 days thereafter. While the word "discovery" is not defined in the policy, the form of notice is therein provided. It is important that the insured make no accusation about employee misconduct without solid information (Malecki, p. 94). Further, the insured should adhere closely to policy requirements about notice and submission of proof of loss statements. Late notice, for example, may be grounds for denial of an otherwise valid claim. If a loss occurs, the insured should work closely with an attorney and his agent/broker at every step in the claims process to ensure that all legal formalities are met and that the carrier's rights are not prejudiced (Henderson and Rodriguez, p. 1). Of course, it is not the intent of the policy to cover employees who committed theft or dishonesty prior to the inception of the policy.

Employee Practices Liability Insurance (EPLI) goes hand-in-hand with crime coverage. When the employer charges the employee with theft and then fires him, the employer is often slapped with a wrongful termination lawsuit. The EPLI policy covers wrongful termination as well as sexual harassment and discrimination. The policies may or may not cover attorneys' fees (Bruegge, p. 13). Before firing the perpetrator the employer should, of course, consult an attorney to help guide him/her through the proper channels. The attorney can also make sure that documentation is prepared before termination that will limit or control damages and possibly avoid lawsuits.

The cost of CCI and EPLI coverage is not great. A small employer with 15 or fewer employees might pay $800 in premium per year for $100,000 of EPLI coverage with a $1,000 deductible. The firm could add $100,000 of commercial crime coverage to its business insurance coverage for only $50 per year. Larger firms would naturally pay more (Bruegge, p. 14).

XI. SUMMARY AND CONCLUSION

Protecting profits is critical to the vitality and survival of businesses both large and small. The problem of employee fraud and abuse has so grown in size and scope that it threatens the underpinnings of business and government. Controlling loss is a continuing challenge to businesses of every size and type. Since dishonesty wears many faces, the thievery may be of many types.

A potential for occupational dishonesty exists when there is opportunity for fraud, the employee has a non-shareable financial problem, and the employee can rationalize his/her theft. The most cost-effective countermeasures to combat internal theft are vigilance in hiring practices and the deployment of loss-control programs such as adequate accounting policies, financial control features, and organizational control features. An essential element in fostering employee compliance with loss-control efforts and harnessing the goodwill and cooperation of employees in identifying thieves in their midst is the tone at and commitment from the top. The importance of the company's beliefs and values should be repeatedly emphasized by management from the date of employee hire to the date of dismissal.

Unfortunately, given recent patterns and trends in the employee theft area, the future seems brighter for the criminal than for the victims. Employee theft is clearly on the rise, and each innovation to prevent or deter workplace theft is met with equally innovative countermeasures as fraudsters continue to come up with new ways of stealing. Given the magnitude of the problem, the potential for improvement is huge, and the company that is successful in preventing or reducing the number of

employee thefts stands to benefit greatly. Reducing fraud helps increase profits, keeps the business running smoothly, and frees up the time of the owner for concentration on his/her vision for the future.

REFERENCES

Association of Certified Fraud Examiners (ACFE), *2006 ACFE Report to the Nation on Occupational Fraud and Abuse*, July, 2006, pp. 1-164.

Anonymous (1), "Employee Thefts Rise," http//web.lexis-nexis.com, October, 2004, p. 11.

Anonymous (2), "Tom Confronts An Ethics Breach," *Gale Group, Inc. Business and Management Practices, Research Technology Management*, Vol. 47, No. 6, November, 2004, p. 56.

Appelbaum, Steven H., Cottin, Jennifer, Pare, Remy, and Shapiro, Barbara T., "Employee Theft: From Behavioral Causation and Prevention to Managerial Detection and Remedies," *Journal of American Academy of Business,* Vol. 9, No. 2, September, 2006, pp. 175-183.

Bruegge, Laura, "Dishonesty Coverages Do Count," *Northwest Arkansas Business Journal*, Vol. 8, No. 5, May 24, 2004, pp. 13-14.

Coenen, Tracy L., "Commentary: The Fight Against Fraud," *Wisconsin Law Journal*, http://web.lexis-nexis.com, April 12, 2006, p. 1.

Coffin, Bill, "Breaking the Silence on White Collar Crime," *Risk Management*, Vol. 50, No. 9, September, 2003, p. 8.

Cressey, Donald R., *Other People's Money: A Study in the Social Psychology of Embezzlement*, The Free Press (Glencoe, IL), 1953.
Dennis, Anita, "The Downside of Good Times," *Journal of Accountancy*, Vol. 190, No. 5, November, 2000, pp. 53-55.

Fishman, Neil H., "Signs of Fraud," *The CPA Journal*, Vol. 70, No. 12, December, 2000, pp. 60-61.

Gips, Michael A., "Workers Paint Shocking Fraud Picture," *Security Management*, Vol. 46, Issue 11, November, 2002, p. 16.

Henderson, Bill, and Rodriguez, Ray, "Employee Theft and Fraud: Get the Facts, Accelerate Recovery," *Corporate Counsel Weekly*, May 19, 2004, pp. 1-2.

Knapshaefer, Johanna, "Deterring Fraud When It's an Inside Job," *Community Banker*, Vol. 13, No. 6, June, 2004. pp. 42-45.

Longmore-Etheridge, Ann, "Bagging Profits Instead of Thieves," *Security Management*, Vol. 45, Issue 10, October, 2001, pp. 70-75.
Lurz, Bill, "Stop, Thief! Are Employees Robbing You Blind?," *Professional Builder*, http://web.lexis-nexis.com, September 1, 2004, p. 112.

Malecki, Donald S., "Who Knew What When?," *Rough Notes*, Vol. 149, No. 3, March, 2006, pp. 94-95.

Mather, Robert, "Protect Investments," *Executive Excellence*, Vol. 18, No. 10, October, 2001, p. 8.

McClurg, Lucy A., and Butler, Deborah, "Workplace Theft: A Proposed Model and Research Agenda," *Southern Business Review*, Vol. 31, No. 2, Spring, 2006, pp. 25-34.

McCormick, Roy C., "Employee Theft Insurance," *Rough Notes*, Vol. 149, No. 5, May, 2006, pp. 122-23.

Meiners, Cary, "Detecting and Eliminating the Unintentional Perk," *Risk Management*, Vol. 5, No. 4, April, 2005, pp. 50-53.

Mohsin, Asad, "A Case of Control Practice in Restaurants and Cafes in Hamilton, New Zealand," Journal of American Academy of Business, Vol. 8, No. 1, March, 2006, pp. 271-276.

Ritter, Bill, "Take The Profit Out of Stealing," *National Petroleum News*, Vol. 96, No. 7, July, 2004, pp. 25, 28.

Ryan, Thomas J., "Nerves of Steel," *Sporting Goods Business*, Vol. 37, No. 6, June, 2004, p. 8.
Schroeder, William, "Fighting Fraud Requires Change in Public Attitude, Stronger Legislation, More Cooperation," *Claims*, January, 1994, pp. 85-86.

Tyska, Lou, "The Thief on Your Payroll," *Pinkerton Solutions*, Vol. 2, No. 1, 1997, pp. 17-19.

Wells, Joseph T., "How to Prevent Employee Theft," *Score*, http://www.score.org, September 3, 2006, p. 1.