ASIS FOUNDATION

# CRISP REPORT

Connecting Research in Security to Practice

# Strategies to Detect and Prevent Workplace Dishonesty

*Read Hayes, PhD*

## ABOUT THE CRISP SERIES OF REPORTS

Connecting Research in Security to Practice (CRISP) reports provide insights into how different types of security issues can be tackled effectively. Drawing on research and evidence from around the world, each report summarizes the prevailing knowledge about a specific aspect of security, then recommends proven approaches to counter the threat. Connecting scientific research with existing security actions helps form good practices.

This series invites experts in specialist aspects of security to present their views on how to understand and tackle a security problem, using the best research evidence available.

Reports are written to appeal to security practitioners in different types of organizations and at different levels. Readers will inevitably adapt what is presented to meet their own requirements. They will also consider how they can integrate the recommended actions with existing or planned programs in their organizations.

This CRISP report focuses on how to prevent employee theft and dishonest behavior. Read Hayes, PhD, discusses the sources of employee theft and a host of prevention opportunities. His recommendations provide solid ideas on how companies can avoid becoming victims of internal theft and how to implement recommended solutions. His discussion will help security practitioners think in a more informed way about deviant behavior among employees.

CRISP reports are based on the Problem Oriented Policing (POP) Guides produced by the Office of Community Oriented Policing Services (COPS) of the U.S. Department of Justice, which can be accessed at www.cops.usdoj.gov. While that series summarizes knowledge about how police can reduce the harm caused by specific crime and disorder problems, the CRISP series focuses on specific problems facing security professionals.

Martin Gill
Chair, Research Council
ASIS International Foundation, Inc.

ISBN-13: 978-1887056-86-1

Printed in the United States of America

CRISP REPORT

Connecting Research in Security to Practice

## An ASIS International Foundation Research Council CRISP Report

# Strategies to Detect and Prevent Workplace Dishonesty

*Read Hayes, PhD*

ASIS International Foundation, Inc. : Alexandria, VA

# Contents

# Executive Summary

Estimates reveal that between 40% and 50% of all business losses can be attributed to employee theft. Employers cannot afford to ignore this large-scale problem and should do everything in their power to create a workplace atmosphere that promotes honesty and encourages and rewards good behavior. They need to make it clear that dishonest behavior will be quickly detected and severely punished.

This report provides research-informed, practical strategies to reduce counterproductive workplace behaviors, including thefts and frauds of all types. It describes factors that can lead to these behaviors, describes common employee theft and fraud methods, and analyzes selected prevention techniques, policies, and technologies.

Regardless of their motivation, many employees are more likely to stray from acceptable behavior when an opportunity presents itself. If an employee perceives little chance of being caught, he or she may be more inclined to steal.

This report provides employers in all types of businesses with ways to discover counterproductive and criminal employee behaviors and to prevent employees from even thinking of swaying from acceptable workplace norms. When implemented, the numerous strategies documented through research can prevent problems from occurring—and reoccurring.

# The Employee Dishonesty Problem

Employees can be a company's greatest asset and, unfortunately, its worst enemy. Counterproductive workplace behavior, or employee deviance, can be defined as intentional behaviors or omissions that not only violate company or public rules but also harm the organization or others. These behaviors and omissions are a pervasive problem for any type of organization and must be controlled.

Asset protection studies indicate the same thing year in and year out: employees account for much, if not most, of a company's losses. Research has shown as many as 75% of all employees have stolen or otherwise harmed their employer (Harper, 1990; Hollinger and Clark, 1983b; McGurn, 1988). Coffin (2003) reports that employee dishonesty is the fastest growing organizational problem for many companies.

Employees have the best access to all company assets. They know where cash is stored. They often need or are able to acquire keys, passwords, alarm codes, and safe combinations (Hayes, 2007). Some company associates, aware of security procedures and systems, believe they are able to accurately weigh their risk of being caught if they steal. More significantly, employees assess the attentiveness of other workers. They know when alert, caring managers and colleagues are present as well as when naïve or apathetic associates are in charge.

Employee theft and error can account for the majority of losses. A recent survey by Hollinger and Adams (2007) reports that retailers believe employees account for 47% of their inventory losses. Employees steal in a variety of ways, but the result is always the same: loss of profits, low morale, and even the demise of an entire business. Regardless of causal factors or excuses, all types of workplace theft and fraud are wrong and harm organizations, other employees, customers, and reputation.

*Employee theft and error can account for the majority of losses. A recent survey reports that retailers believe employees account for 47% of their inventory losses.*

# The Workplace Dishonesty Spectrum

Aberrant employee behavior encompasses a range of actions; one end of the spectrum includes undesirable and perhaps unintentional behaviors like tardiness, chronic absences, or errors resulting from inattention to detail. Employees may ignore customers, spread rumors, misuse computers or the Internet, or even sabotage software or property. More harmful behaviors include interpersonal problems like rudeness, threats, and attacks. However, purposeful actions such as theft and fraud provide the most frequent harm to businesses.

Every work environment is vulnerable to the negative effects of counterproductive and even deviant employee behavior. The retail industry, for example, is particularly vulnerable to employee theft because stores display and sell physical merchandise. Every type of retail organization—from cosmetics boutiques to auto parts factories to post offices—carries assets that can be unlawfully removed by company employees.

Cleaning crews removing trash or supplies are in an excellent position to carry merchandise to their vehicles or to those of accomplices. Employees have been known to damage merchandise intentionally and mark it out-of-stock, an indirect means of theft. Employees may shoplift or give away merchandise. Fraudulent returns, robberies, and gas drive-offs can also involve retail employees.

Every organization has its own unique risks. Drugstores carry prescriptions that contain controlled substances, which must be carefully guarded. Grocers experience both employee and customer "grazing," or the eating of merchandise. Transportation companies can suffer hijackings perpetrated by employees. Offices experience embezzlement, interpersonal harassment, and employees stealing from each other. Manufacturers and distribution centers stock materials and finished goods, which are vulnerable to theft and diversion. Product buyers may collude with suppliers to siphon off funds. Accountants may embezzle, and employees may threaten each other.

*Employees have been known to damage merchandise intentionally and mark it out-of-stock, an indirect means of theft. Employees may shoplift or give away merchandise.*

# Factors Contributing to Workplace Dishonesty

A review of research on workplace theft can provide insight into the reasons why employees steal from their employers. While employees may deviate from expected norms for a variety of reasons, researchers have identified two major causes: personal issues and situational or environmental factors (Mikulay, Neuman and Finklestein, 2001, Robinson and O'Leary-Kelly, 1998).

Personal issues that predict dishonesty appear to account for a relatively small but important amount of the variance in predicting deviant behavior among workers (Martinko, Gundlach and Douglas, 2002; Ones, Viswesvaran and Schmidt, 1993). They include greed, skewed personality traits, low cognitive ability, and limited self-control. Another factor can be tolerant or conditional attitudes toward unacceptable behaviors. An employee might think that taking less than $25 is not wrong, for example, but taking more is (Bolin and Heatherly, 2001; Dilchert et al., 2007; Terris and Jones, 1980).

Another personal issue involves the perception by employees of a low or non-existent risk of detection and sanction. This attitude may account for much of the variance in the probability that an offending action will occur. (Ajzen, 1991; Greenberg and Barling, 1996; Hollinger and Clark, 1983; Murphy, 1993).

Situational or workplace factors that lead to employee thefts can include wanting to be accepted by a worker-related gang, an apathetic work group, or an influential peer. Overwhelming workplace pressures, wanting to satisfy immediate needs or desires, feeling left out or abused, and conforming to or tolerating dishonest group behavior can lead employees to commit or participate in thefts. Employees can be motivated to steal by watching their leaders and peers break the rules or because they feel somehow abused or overlooked.  In other cases, employees steal to acquire prestige or notoriety.

Research explains that workplace deviance results from the interaction between misguided individuals and their workplace. However, researchers still do not understand how or when an environment or situation triggers or enables a deviant act or whether a motivated offender just takes advantage of a favorable theft situation (Henle, 2005).

Deviant behavior is sometimes simply impulsive. Many cases simply arise from a need or desire: the employee may just want a certain item or require money for specific needs like bills, drugs, a relationship, an upcoming event, or everyday expenses.

Employees can convince themselves that dishonesty is a form of compensation or retribution. If an employee feels he or she is not being fairly compensated or is overworked, he or she may view dishonest behavior as a way to even the balance (Greenberg, 1990).  Sometimes employees believe working for a big company or nationwide chain means cash or merchandise won't be missed.

Committing crimes against an employer can also partially result from feelings of anger toward a supervisor, coworker, or the company as a whole. To underscore this point, research has shown that managers may contribute to unacceptable workplace behaviors because they influence the following business practices and attitudes (Litzky et al., 2006, etc.):

1. Compensation and rewards
2. Social pressures to conform
3. Negativity and distrust
4. Ambiguity about job performance
5. Unfair treatment
6. Access to assets and risk controls
7. Employee trust

In summary, persons prone to negativity, unable to control impulses, with a perceived need for money, surrounded by uncaring or dishonest peers, under pressure, believing theft is acceptable under certain conditions, believing their boss is a jerk, and with access to unguarded assets are likely to steal (Hayes, 2007). Figure 1 is a simplified model of this premise.

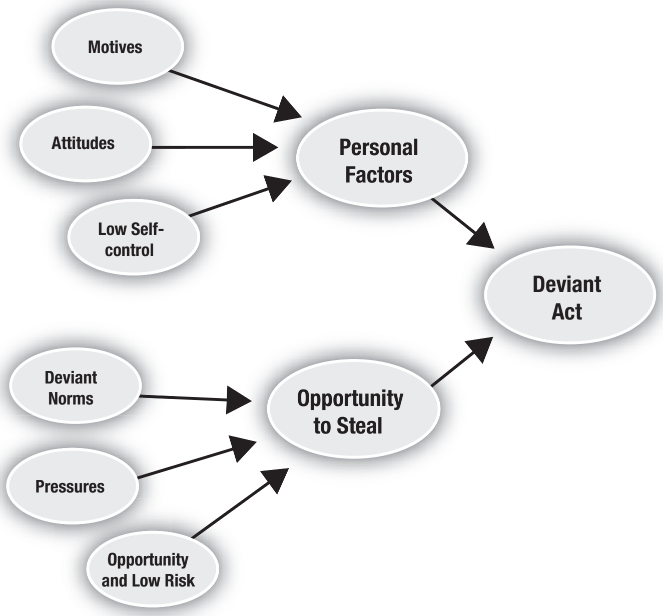

**Figure 1. Interaction of Workplace Environment and Personal Factors**

# Conditions Enabling Employee Deviance

Based on theories of high-risk workplace behaviors developed through research, organizations should compile a checklist of conditions in each of their locations to help gauge the likelihood of deviance reflected by increased risk and vulnerability. A sample checklist of questions that can determine vulnerability is shown in Appendix A.

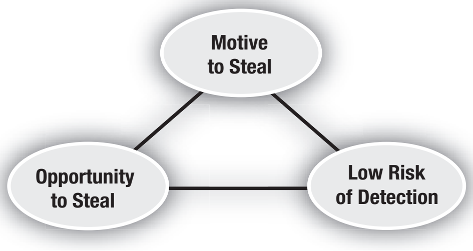

**Figure 2. Theft Triangle**

To tie together the theoretical literature and create a workplace action model, the theft triangle, as shown in Figure 2, was developed (Hayes, 1997). This model hypothesizes that certain conditions must be present before an employee can initiate or facilitate a successful theft.

Loosely modeled on the fire triangle, the theft triangle illustrates three factors: motive—the potential gain and uses of a given asset; opportunity—the ability to quickly and safely remove the asset from its location; and personal risk—the probability of being caught and severely punished if perpetrators steal the asset. Of course, not all offenders consider each factor every time they contemplate stealing, but the model provides a useful tool for understanding motivation.

Asset protection is all about convincing thieves that they should go somewhere else. The theft triangle helps any loss prevention manager do just that. Would-be offenders consider, balance, and reconcile threatening cues before and after arriving at a location. These cues are a combination of facilitators (which can make theft easier) and deterrents (which make thefts tougher or riskier). The theft triangle can be used to focus loss prevention efforts since it is based on criminal perceptions.

# The Crime and Loss Control Process

Crime and loss control, like any problem-solving exercise, is a process. Unacceptable behavior among employees is a long-term issue for any organization. Businesses should strive to implement a standardized three-part decision-making process before implementing countermeasures.

**Diagnose.** Use CCTV footage, shrinkage data, employee reports, audit scores, incident reports, peer reporting, employee surveys, and apprehended offender interview data to define the problem's dynamics, patterns, and opportunities.

**Prescribe.** Take a diagnostic approach to uncover people, programs, and places that deserve special attention. Procedures and technologies can be implemented using the Theft Triangle in Figure 2 to increase the perceived risk of detection, decrease access to and the mobility of critical assets, and affect the motives and rationalizations of offenders. An example of a prescribed control program is shown in Appendix B.

**Test and Refine.** Asset protection protocols should be tested and refined using inventory and cash counts, sales data, CCTV footage, incident reports, and employee and offender feedback.

# A Culture of Honesty

As discussed earlier, research on employee dishonesty indicates that situational factors are a critical part of creating a climate where employee deviance can fester (Applebaum et al., 2006; Bennet and Robinson, 2003; Greenberg, 2002b). As a result, the culture and norms of a workplace are important to organizational success (Tomlinson and Greenberg, 2005). Companies should strive to establish a culture of honesty by establishing a code of conduct that sends an explicit message to all employees that honesty will be rewarded and dishonesty will not be tolerated (Dunn and Schweitzer, 2005; Vardi and Weitz, 2004).

Employers should ensure that all employees are aware of both corporate standards for behavior and the benefits that result from upholding those standards (Navran, 1997). In addition, all employees in the organization, from the CEO down, should be aware of the security risks faced by the company, the actions they can personally take to reduce and report loss incidents, and the potential rewards for doing so (Hayes, 1993). Employees must also understand that thefts or any violations of company policy, at any level, will initiate a three-tiered result: a fair hearing; swift, consistent, and serious sanctions; and the potential for termination, criminal prosecution, or civil action (Hollinger and Clarke, 1982).

Many loss prevention techniques—such as transaction and other exception monitoring, education programs, and fraud assessment questioning—can help reduce employee thefts. However, one of the most effective techniques is to have employees monitor and report the suspicious, illegal, or unethical behavior of other employees (Miethe, 1999). Coworkers are more likely to be aware of activities that might otherwise be difficult to uncover, and they can detect their peers' dishonest or suspicious activities more quickly than exception software, financial audits, or exit interviews.

Employees are more likely to report others if the work environment makes it clear that theft or other violations are not acceptable behavior. In fact, employee monitoring may be among the most cost-effective ways of reducing shrinkage. Techniques to encourage employee monitoring include telephone hotlines and incentive or award systems. Even creating an environment that expects employees not only to work hard and have fun but also to monitor and report the illegal or suspicious activities of other employees has proved to be successful (Scicchitano, Johns, Hayes, and Blackwood, 2004).

Management should be aware that many honest employees may be unwilling to "snitch" on friends or colleagues. To overcome this reluctance, employees should be assured that hard work and ethical behavior are the standard. They should also clearly understand that the identity of anyone who reports dishonesty, theft, or deviance on the part of another employee will be held in strict confidence. To this end, a toll-free, 24-hour hotline to facilitate the reporting of theft, fraud, substance abuse, or sexual harassment in the workplace is important. Companies may use an outside service or set up an in-house hotline. In either case, offering monetary incentives, such as a gift certificate or gift card, can both encourage employees to participate and reward them for doing so.

Communication is an important part of maintaining a positive and honest work environment (Navran, 1997). When employees feel unable to communicate their concerns, ideas, and problems to upper management, morale plunges and thefts and errors increase. Supervisors at all levels must be taught to communicate effectively with their staffs—and be rewarded for doing so. The CEO should have an open line of communication to all employees. A confidential written suggestion format often works well in accomplishing this goal.

Finally, supervisors, managers, and executives must always lead by example (Hayes, 2007). Persons who have difficulty being a leader should be identified and counseled so they can become part of the team, helping to inspire other employees to achieve the expected norms of hard work and ethical behavior.

# Preemployment Screening

Successful businesses address employee dishonesty and theft using an integrated process, and one of the most important parts of that process is preemployment screening. No one can absolutely predict what another person will do in a particular situation, but knowing how an applicant acted in a previous workplace or in other decision-making roles can help. Past behavior can be a strong indicator of future actions. That is what background screening is designed to do—help managers predict a prospective employee's workplace behavior.

Background checks are a way to find positive or negative issues from previous employers. Also, frequent driving violations, criminal convictions, multiple worker compensation filings, and falsification of educational degrees or professional licenses are all risky behaviors and should be a red flag for a future employer. To get facts, employers should contact work references, asking for some indication they would re-employ the individual. Just contacting personal acquaintances is insufficient.

### Methods for Accurate Hiring Decisions

Hard work, collegiality, and integrity are keys to keeping a company's performance level high. Keeping in mind the desire for honest, agreeable, and hard-working staff, the company's screening program should look for indicators of all three. A combination of the following methods and actions will help employers gain a more complete picture of a prospective employee and provide support for hiring decisions.

**Application Screening.** Potential hires should be asked to complete an employment application. The application form should conform to all current legal standards. Any gaps in employment or ambiguous responses should be questioned. Many employers also require applicants to present identification documents.

*Frequent driving violations, criminal convictions, multiple worker compensation filings, and falsification of educational degrees or professional licenses are all risky behaviors and should be a red flag for a future employer.*

**Personal and Professional Reference Checks.** Any individuals the applicant lists as references should be contacted and queried. The applicant should be discussed in a positive manner, and the name and phone number of other acquaintances should be solicited for further reference. The identity of the person acting as a reference should also be verified.

**Employment and Education Verification.** All jobs, training, and education listed on the application should be checked. When reviewing past employment history, a rule of thumb is to go back three to five years. If the job for which the individual is applying requires a certain level of education or a certification, have the applicant sign an authorization allowing colleges and schools to release transcripts.

**Integrity Interview/Scenarios.** Each applicant should be interviewed at least twice, preferably by two different interviewers. The interviewers should ask open-ended questions, allowing applicants to discuss their thoughts and ideas. Courses and books can help sharpen an interviewer's ability to determine if a subject is being truthful or deceptive. Some retailers, after gaining legal validation, put applicants in a simulated work or decision-making situation and observe their performance. This practice also gives applicants a feeling for the job for which they are applying.

**Written Honesty or Aptitude Tests and Self-Report Surveys.** Since the polygraph is no longer legally valid as a screening tool, many states are allowing the use of pencil-and-paper tests or surveys to determine honesty. Some of these tests, for example, rely on empirical research to predict future behavior based on applicants' past risk-taking or rule-breaking behavior or their tolerance for types or levels of dishonesty.

**Background Checks.** Many retailers use in-house personnel or contractors to check the criminal conviction and credit history of applicants for positions that require this type of information. Employers also frequently check workers' compensation claims and driving records. Books and software programs are available to assist retailers in these types of checks. In addition, an Internet search can locate national organizations that can provide guidance, such as the National Retail Federation and ASIS International. Most states also have a retail merchants association that can help at the local level.

# Retail Controls and Audits

Another way to prevent and manage aberrant employee behavior is to establish workable controls with relevant and effective follow-up. Procedural or operational controls are designed to affect the Theft Triangle shown in Figure 2 by reducing motives and opportunity for crime while increasing potential offenders' perceptions that they risk being detected and severely sanctioned (Hayes, 2007).

The nature of retail businesses makes them especially prone to incidents of employee dishonesty. When designing control procedures, however, retailers should keep in mind operational (or "real world") employee and customer service activities to avoid impeding the normal flow of business. If cumbersome procedures drive away good customers, they will be abandoned quickly by company employees.

Appendix C lists 25 measures that retail businesses can use to monitor and prevent unacceptable workplace behaviors. In addition, the following merchandise, cash, and audit controls have been found to be successful in retail settings.

### Merchandise Controls

These products, policies, and strategies have proven to be most effective in maintaining oversight of merchandise:

**High-tech tags.** Electronic article surveillance (EAS), radio frequency identification (RFID), benefit denial tags, and electronic, dye, or mechanical tags can be attached or concealed inside high-loss assets as a theft deterrent.

**Spot audits and counts.** Unannounced audits or selected merchandise piece counts can detect and deter employee pilferage. These practices put employees on notice that management closely tracks the company's assets. High-loss items should be the focus of special counting and security (Masuda, 1992), while posting the loss levels of these items in employee break rooms will help cut thefts (Carter et al., 1988).

**Receiving and pick-up policy.** Receiving doors should be properly secured when not in use, and all receiving and customer pick-up activity should receive management oversight. Delivery personnel should be observed at those locations.

**Purse and package checks.** A policy allowing management or security to check employee purses or packages when exiting the workplace should be in place. To be effective, the reasons for this policy should be made clear to all employees and be applied consistently.

**Trash removal and cleaning crew monitoring.** In-house, contract, or vendor managers should observe the removal of trash and containers (in clear bags when possible). Keeping dumpsters locked and employee parking away from rear exits and trash areas may also reduce theft opportunities.

**Damaged and returned merchandise.** All merchandise slated to be destroyed, returned to its vendor, or donated to charity must be logged in and secured in a locked, wire enclosure until it is disposed of. These methods can help avoid employee pilferage or fraudulent refund schemes.

**Employee discount and purchase control.** All employee purchases should be entered in a log with the employee's signature, or tracked electronically. To receive a discount, employees and their immediate family members should present valid company identification cards.

### Cash Controls

In many organizations, employees must handle cash, which can be a cause for concern unless specific controls are established, implemented, and audited. The following suggestions can help companies of all types maintain control of cash on their premises.

**Register accountability.** Only a few employees should be assigned to one register simultaneously, and only one at a time if possible. All employees should log in their employee number when entering a transaction. These two policies can help to reduce cash overages and shortages and quickly determine who may be responsible for missing cash.

**Electronic or physical register data review.** Exception-reporting software should be used to randomly check journal tapes and ledger sheets from point-of-sale terminals and cash registers to uncover errors or questionable practices. Training and skill deficiencies may be detected as well.

**Post-void authorization and follow-up.** At times, clerks need to legitimately void all or part of a transaction. This activity should be checked by a manager as soon as possible to see whether the purchases were re-entered correctly. If a customer decides not to purchase a selected item while at the check-out, find out where the clerk stored it. Also, track post-voids for trends, such as reasons for voids or clerk employee numbers.

**Cash refund authorization and follow-up.** Customers should supply their name, address, and phone number as well as sign a refund slip to receive a cash refund. Multi-part forms that are numerically issued and logged can be used for this purpose. One copy should be given to the customer, one copy should remain with the returned merchandise, and the third copy should be sent to the cash office. When the merchandise is returned to the sales floor, the clerk returning the item should sign under the issuing clerk's signature. If the transaction is above a predetermined amount, a manager should personally authorize the transaction.

**Tracking cash variances.** All cash overages and shortages should be posted so trends can be determined. If no patterns are apparent, a "shotgun" shortage exists, and a manager or head clerk with access to all registers may be responsible.

**Tracking price variances.** An automated price tracking system can be an enhancement to any operation. As an alternative, a manual or automated system that tracks transactions below purchase price is recommended. A clear pattern of low or high price ring-ups may indicate intentional under-ringing or manipulation.

**Deposit verification.** Cash office personnel should be taught the proper way to count money. Using a calculator with a non-add key, deposits should be counted once and totaled by denominations. This information should be entered on the adding machine tape along with the date. The clerk should then recount the deposit in the same manner and compare the total with the previous total documented on the tape. If the totals are the same, the clerk should initial and date the tape. A manager should then repeat this process and staple these tapes to a copy of the deposit receipt and save them for recordkeeping purposes.

**Test-shoppers and seals.** "Visitors" should be used to test cash and other transactions while also randomly observing the integrity of item picking, packing, shipping, and receiving. Truck seals should be used on all transports and product shipping tubs containing items with high loss records.

### Process audits

Audits of cash and merchandise-handling procedures should be conducted to determine if proper controls are in place and being followed, and to determine if and where problems exist. Audits should be conducted randomly, after the manager overseeing the procedure is briefed on what processes and materials are going to be checked and how they will be inspected. Managers should also know why the audit is necessary before it commences. Ideally, audits should check all asset protection processes from a store's entrances, through points of sale, to storage areas, exits, cash handling rooms, employee lockers, and all other places where exceptions could occur.

# Retail Fraud

Retail businesses are also frequent victims of employee fraud. Eleven ways to counter fraud problems in retail settings are shown in Appendix D. In addition, the following types of retail fraud deserve extra attention and unique solutions.

## Gift, Debit, and Credit Card Fraud

The use of gift cards continues to grow, providing retailers with a powerful sales and branding tool. However, employees can take advantage of this payment method by acting alone or in collusion with others. They can attempt to steal "live" cards that have been left behind or lost, to purchase cards with stolen or counterfeit cards, to use random number programs when making gift card purchases, or to clone or counterfeit cards. To uncover possible fraud, businesses should monitor users for patterns, track customer complaints, and use anti-counterfeit symbols on their cards. Credit card purchases of large gift card denominations should also be noted.

Credit card fraud takes many forms. Employees can engage in such devious acts as crediting a friend's card with returned merchandise refunds, opening company credit card accounts for fictional people, or making their own charges on a customer's card number. Retailers can reduce fraud attempts by using charge exception reports along with unique chips and PINs.

## Coupon and Loyalty Card Fraud

Businesses often use loyalty cards and Internet site promotions to keep their customers actively involved with their stores. Discount coupons and gift coupons also create customer goodwill and provide incentive for customers to spend more time and money in stores or the retailer's website. However, these marketing tactics can provide opportunities for employee or collusive fraud. Those opportunities can be controlled by tracking and monitoring the printing and issuing of cards, coupons, and special codes.

## Refund Fraud

In today's "hassle-free" customer service environment, retailers are especially vulnerable to refund fraud. Customers expect to exchange or return merchandise easily, but nefarious employees can easily take advantage of lax refund policies. The challenge is to keep legitimate customers happy while also preventing fraud.

Refund fraud can happen in a number of ways. For example, suppose employees decide they need cash immediately and do not want to "till-tap" or void a transaction. Using a refund slip or the point-of-sale system, and a false name and address, employees can complete the return information. They simply record the amount of cash they desire as a refund, sign and date the slip, then substitute it for cash. Or, they credit their accounts, or the credit card of an accomplice.

Some refund fraud countermeasures include numbering refund slips and logging them out as needed. As an added precaution, a manager should always authorize refunds greater than $100. Electronic marking of products with Internet tracking tools or refund listing services also provides notification and flags the patterns of refund fraudsters.

Customers should be required to sign a refund slip, which should also be signed by the issuing clerk and the employee who returns the merchandise to the sales floor. Managers should randomly call customers who returned merchandise and inquire if the transaction was handled to their satisfaction. This action is not only a positive customer service strategy, but may expose a dishonest employee if a "customer" claims never to have been in the store.

On the other hand, managers should always pass along positive customer comments to store employees, preferably in a group meeting. These comments not only recognize the courteous employee but also reinforce the message to staff that management is checking refunds and returns.

### Layaway Fraud

Many stores have layaway plans; this is another customer service from which dishonest employees can steal. The three most common methods to steal via layaways involve voiding a layaway payment, canceling a layaway transaction, and forfeiting a layaway deposit. To prevent employees from engaging in these tactics, a manager's authorization should be required to prevent fraudulent layaway cancellations or payment voids. Similarly, a manager should authorize all deposit transactions.

### Embezzlement and Other Frauds

The term "embezzle" refers to the stealing of company money by someone in a position of trust. Retail embezzlement can occur at any level of the organization. Cash register theft is one form of embezzlement; others include bank deposit rolling, check kiting, lapping, payroll fraud, travel and expense account fraud, as well as vendor kickbacks and collusion.

**Bank deposit rolling.** This type of crime is not particularly common. Rolled bank deposits usually occur in stores where employees make up the daily sales receipts for deposit. In this type of embezzlement, the employee steals all or part of the day's deposit, making up for the stolen cash with monies from future deposits. It can easily be prevented by having separate employees verify each day's deposit on a rotating basis.

**Check kiting.** In this type of fraud, employees authorized to write checks or make deposits in two or more bank accounts may attempt to "kite" or float funds between a legitimate account and one set up by the employee or an accomplice. Once a check from the company is deposited into the bogus account, the employee makes a withdrawal of cash in that same amount. Before the original check clears the company's account, the employee deposits a check from his account into the company's to cover the original account. This cycle continues until the scheme breaks, when either the company or one of the banks refuses to honor the checks. This illegal activity can be thwarted by having two supervisors sign off on checks and by reconciling checking accounts at least monthly.

**Lapping.** In lapping schemes, dishonest employees keep part of the payments made on accounts received. This method is similar to deposit rolling, because parts of other payments are skimmed to cover the loss. Account records and statements are altered by the employee. This type of crime can go undetected for years. To avoid this type of theft, a manager should verify and approve all bank deposits.

**Payroll and fake vendor or accounts payable fraud.** Payroll fraud often occurs when an employee with the access and authority to add employees to payroll adds fictitious employees or vendors to the roster. Paychecks are then issued either to the dishonest employee or to an accomplice. To avoid this scheme, retailers should divide payroll functions among at least three people who prepare, verify, and distribute payroll. Employee and vendor payroll rosters should be approved by a manager, then audited and updated quarterly.

**Travel and expense account fraud.** Employees are traveling more and more for business, which means expense reports and accounts have become prime targets for fraud. Employees typically list personal expenses such as meals and telephone calls on reports, which are submitted for reimbursement. To avoid fraud, companies should employ and publicize firm policies regarding legitimate expenses. Appropriate supervisors should then verify and authorize all submitted expense reports.

# Other Types of Business Abuses

Another category of internal theft includes many types of fraud that can occur at all levels and in every department of a company. A significant method of employee theft involves filing false workers' compensation claims, for example. This practice may now be replacing unemployment claims as a desirable source of income. Management should investigate all worker compensation claims to determine if abuse is occurring.

A variety of individuals, such as unsupervised work crews, laid-off employees, and disgruntled staff, may inflict damage on a business in the form of vandalism or sabotage. Distribution of company assets and work stoppages can lead to this type of risk. To avoid such situations, supervisors should keep lines of communication open to determine if morale problems exist. They should also debrief terminated or laid-off employees prior to departure to inform them of company policies and deny them access to sensitive areas on the company's property.

Every business is vulnerable to theft by cleaning crews. Therefore, it is essential to supervise in-house or contract cleaning personnel. Random checks of toolboxes, cans of wax, vacuum cleaner bags, and trash are a must to be sure cleaners are not participating in deviant behaviors.

Employee pilferage of company supplies and equipment is also a form of theft. Tools, office equipment, and supplies disappear from businesses at an alarming rate. This type of theft may occur sporadically or in an organized manner. All employees should be made aware of the company policy regarding "using" or "borrowing" company assets for personal endeavors. Management should inventory and permanently mark valuable items, and secure sensitive areas to help control this type of loss.

Other abuses faced by businesses today include unethical conduct, time theft, substance abuse, and the compromising of proprietary information.

## Unethical Conduct

Business ethics are under increased scrutiny as more well-known government and private enterprises face criminal indictment. In a business, most key employees are in a position to accept a bribe or kickback from a product or service vendor. Merchandise buyers, travel agents, purchasing agents, shipping traffic managers, in-house agents, new store and distribution center real estate locators, and in-house construction supervisors are just some of the individuals in positions to recommend or authorize agreements with outside vendors. Organizations can reduce their vulnerability to this type of crime by considering some the 13 actions show in Appendix E.

### Time Theft

The theft of time is another fraud that can occur within all types of businesses. Time theft occurs when an employee clocks in for another employee who is late or absent, calls in sick for a paid day off, leaves early, takes long breaks, or uses the company's time to conduct an outside business. Positive leadership practices by supervisors, including good discipline, two-way communication, and positive morale all help control time abuse.

Retailers have used several methods to counter this potential fraud. In an effort to make employees feel that they are a significant part of their company, many retailers offer employee discounts on store merchandise. These programs can boost employee morale and contribute to a sense of belonging to a team. Employee discounts can average around 10% on low-margin items and 20% on others. However, to avoid fraud, any discount policy should be in writing and monitored by store managers.

### Substance Abuse

In today's society, alcohol and drug abuse constitute tremendous threats to the safety and security of any organization. Drug-addicted or alcoholic employees can increase the number of workplace accidents and thefts. Employers should screen applicants to keep individuals with untreated addictive or criminal tendencies from entering the company workforce. Companies can face serious liability if substance-dependent employees are untreated. Severe losses, injuries, or even death can result.

Some businesses even place undercover agents within their operation to determine the source of substance abuse activity related to an increase in thefts.

Supervisors should be trained to detect problem employees and refer them to Employee Assistance Programs (EAP), which have been shown to be extremely effective by government and private experts.

### Protecting Proprietary Information

All operations possess proprietary, or sensitive, information. This can include corporate expansion goals or locations, sales figures, and customer mailing lists. All proprietary information may be confidential, but all confidential information may not be proprietary. Personnel and training files are confidential, but are not considered proprietary. Businesses must ensure that confidential information is carefully guarded.

A company's trade secrets may be subject to greater protection under federal law if the company can show that it makes reasonable efforts to maintain their secrecy, such as classifying specific types of documents as confidential and notifying employees of the actions it will take against breaches of confidence. An employee can seriously undermine a company if he or she divulges trade secrets, either intentionally or accidentally.

A basic proprietary information security plan should include the following steps:

1. Non-employees should be restricted from accessing areas containing confidential information.

2. Warning signs and instructions should be posted to alert employees to sensitive objects or places.

3. Employees and visitors should be informed that certain information is confidential.

4. Sensitive documents should be stored separately in containers for which special security precautions are taken.

5.  Access to sensitive areas within a facility should be controlled to differentiate among different classes of employees with respect to their ability to handle certain information or operations.

6. Employees and suppliers should be instructed not to disclose information entrusted to them to other employees, unless such employees present a legitimate "need to know."

# Investigating Employee Theft

Management can uncover employee pilferage or embezzlement in a variety of ways, such as performing spot audits and gaining information supplied by an accomplice or witness. A third important strategy is to conduct follow-up investigations on inventory shortages, gross margin problems, price variances, discount issues, gift card and credit card patterns, cash variances, and high-risk transactions such as refunds and voids.

Loss prevention personnel should vigorously investigate all accusations and indications of theft activity. The investigator should be a neutral third party, who should approach investigations with an open mind. Investigators should work closely with colleagues in human resources, personnel, and operations; the resulting cooperation and interdisciplinary expertise will benefit the investigation as well as future deterrence efforts.

The goals of any investigation are to confirm or reject the accusation; discover the extent of any damage or loss, as well as employee involvement; recover lost assets; determine the circumstances that initially led to the incident for future prevention efforts; and provide evidence for sanctioning.

The normal investigative routine is to first gather evidence of wrongdoing through reviews of documentation and surveillance data. Next, the investigator should create a hypothesis about what happened and how it occurred, generate a list of suspects, narrow the list, and conduct preliminary interviews. Once the source of the theft is discovered, the investigator should determine whether enough evidence is present to take action (such as termination, criminal prosecution, or civil action). Conversely, a lack of evidence might mean the investigation should be suspended or dropped.

Investigations must be handled with professionalism and confidentiality, or the company can face serious liability. All implicated employees must be presumed innocent until proven otherwise. Thorough investigations should be conducted in an environment that stresses employee dignity and rights.

Only violations of the law or company policy should be investigated, meaning that certain activities, such as union organizing, are not typically a reason to initiate investigations.

# Future Research Needs

The workplace deviance literature cited in this report provides guidance on causal factors involving personal and situational characteristics that can lead to problems for employers. But more research is needed to uncover how these two main factors are linked.

In addition, future research should evaluate what prevention methods apply specifically to the workplace. Greenberg (2004) and others have done a good job using laboratory and student research or field evaluations (Carter et al., 1988; Masuda, 1992; Mishra and Prasad, 2006). But more rigorous research is needed on employee-related, anti-theft strategies to determine the efficacy and cost-effectiveness of such methods as preemployment screening, the culture of honesty, and process controls.

Researchers have found the following actions to be the most promising: screening applicants for employment; maintaining a positive and honest workplace environment; establishing controls; and taking consistent, but tough action against transgressors.

But more in-depth research is needed to support the theory that combinations of actions offer the best chance for limiting the frequency and severity of inevitable employee problems.

With collaborative goals in mind, employers and researchers alike can work together to create a healthy and productive workplace.

# References

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50, 179–211

Appelbaum, S. H., Cottin, J., Pare, R. and Shapiro, B.T. (2006). Employee theft: From behavioral causation and prevention to managerial detection and remedies. *Journal of American Academy of Business* 9, 2, 175–182.

Bolin, A., and Heatherly, L. (2001). Predictors of employee deviance: The relationship between bad attitudes and bad behavior. *Journal of Business and Psychology*, 15, 405–418.

Carter, N., Holmstrom, A., Simpanen, M., and Melin, L. (1988) Theft Reduction in a Grocery Store through Product Identification and Graphing of Losses for Employees. *Journal of Applied Behavior Analysis*, 21(4), 385–389.

Coffin, B. (2003, August). Breaking the silence on white collar crime. *Risk Management*, 40.

Dilchert, S., Ones, D.S., Davis, R.D., and Rostow, C.D. (2007). Cognitive ability predicts objectively measured counterproductive work behaviors. *Journal of Applied Psychology,* 92(3), 616–627.

Dunn, J., and Schweitzer, M. E. (2005). Why good employees make unethical decisions: The role of reward systems, organizational culture, and managerial oversight. In R. E. Kidwell Jr. & C. L. Martin (Eds.), *Managing organizational deviance* (pp. 39–68). Thousand Oaks, CA: SAGE Publications.

Greenberg, J. (1990). Employee theft as a reaction to underpayment inequity: The hidden cost of pay cuts. *Journal of Applied Psychology*, 75, 561–568.

Greenberg, J. (2002b). Who stole the money, and when? Individual and situational determinants of employee theft. *Organizational Behavior and Human Decision Processes*, 89, 985–1003.

Greenberg, L. and Barling, J. (1996). Employee theft. *Journal of Organizational Behavior*, 46–64.

Harper, D. (1990). Spotlight abuse- save profits. *Industrial Distribution*, 79, 47–51.

Hayes, R. (1993). Employee theft control. Orlando: Prevention Press.

Hayes, R. (1997). Retail crime control: A new operational strategy. *Security Journal*, 8, 225–232.

Hayes, R. (2007). *Retail security and loss prevention*, (2nd ed.). London: Palgrave Macmillan.

Henle, C.A. (2005). Predicting workplace deviance from the interaction between organizational justice and personality. *Journal of Managerial Issues*, 17(2), 247–263.

Hollinger, R.C. and Adams, A. (2007). *National retail security survey*. Gainesville, FL: University of Florida.

Hollinger, R.C. and Clark J.P. (1982). Formal and informal social controls of employee deviance. *The Sociological Quarterly,* 23(3), 333–343.

Hollinger, R. C., and Clark, J. P. (1983a). Deterrence in the workplace: Perceived certainty, perceived severity, and employee theft. *Social Forces*, 62, 398–418.

Hollinger, R. C., and Clark, J. P. (1983b). *Theft by employees*. Lexington, MA: Lexington Books.

Litzky, B. E., Eddleston, K. A., and Kidder, D. L. (2006). The good, the bad, and the misguided: How managers inadvertently encourage deviant behaviors. *Academy of Management Perspectives*, 20, 91–103.

Martinko, M.J., Gundlach, M.J., and Douglas, S.C. (2002). Toward an integrated theory of counterproductive workplace behavior theory: A causal reasoning perspective. *International Journal of Selection and Assessment*, 10(1/2), 36–50.

Masuda, B. (1992). Displacement and diffusion of benefits and the reduction of inventory losses in a retail environment. *Security Journal*, 3, 131–136.

McGurn, J. (1988, March 7). Spotting the thieves who work among us. *Wall Street Journal*, A16.

Miethe, T.D. (1999). *Whistleblowing at work: Tough choices in exposing fraud, waste, and abuse on the job*. Boulder, CO: Westview.

Mikulay, S., Neuman, G., and Finkelstein, L. (2001). *Counterproductive workplace behaviors. Genetic, Social, and General Psychology Monographs, 127, 279–300.*

Mishra, B.K and Prasad, A. (2006). Minimizing retail shrinkage due to employee theft. *International Journal of Retail and Distribution Management*, 34(11), 817–832.

Murphy, K. R. (1993). *Honesty in the workplace*. Pacific Grove, CA: Brooks Cole.

Narvan, F. (1997). *Twelve steps to building a best-practices ethics program*. Workforce, 76, 117–122.

Ones, D. S., Viswesvaran, C., and Schmidt, F. L. (1993). Comprehensive meta-analysis of integrity test validities: Findings and implications for personnel selection and theories of job performance. *Journal of Applied Psychology*, 78, 679–703.

Robinson, S.L., and O'Leary-Kelly, A.M. (1998). Monkey see, monkey do: The influence of work groups on antisocial behavior. *Academy of Management Behavior*, 41(6), 658–672.

Scicchitano, M., Johns, T., Hayes, R., and Blackwood, R. (2004). Peer reporting to control employee theft. *Security Journal*, 17(2), 7–19.

Terris, W., and Jones, J. (1980). Attitudinal and personality correlates of theft among supermarket employees. *Journal of Security Administration*, 3(2), 65–78.

# Bibliography

Tomlinson, E. C., and Greenberg, J. (2005). Discouraging employee theft by managing social norms promoting organizational justice. In R. E. Kidwell, Jr. & C. L. Martin (Eds.), *Managing organizational deviance* (pp. 211–236). Thousand Oaks, CA: SAGE Publications.

Vardi, Y., and Weitz, E. (2004). Misbehavior in organizations: *Theory, research, and management*. Mahwah, NJ: Erlbaum.

Ambrose, M. L., Seabright, M. A., and Schminke, M. (2002). Sabotage in the workplace: The role of organizational injustice. *Organizational Behavior and Human Decision Processes*, 89, 947–965.

Andersson, L., and Pearson, C. (1999). Tit for tat? The spiraling effect of incivility in the workplace. *Academy of Management Review*, 24, 452–471.

Ashforth, B. (1997). Petty tyranny in organizations: A preliminary examination of antecedents and consequences. *Canadian Journal of Administrative Sciences*, 14, 126–140.

Astor, S. (1972). Twenty steps for preventing theft in business. *Management Review*, 61, 34–35.

Aquino, K., Galperin, B.L., and Bennett, R. (2004). Social status and aggressiveness as moderators of the relationship between interactional justice and workplace deviance. *Journal of Applied Psychology*, 34, 1001–1029.

Baumer, T. L., and Rosenbaum, D. P. (1984). Combating retail theft:  Programs and strategies (pp. 115–124). Stoneham, MA: Butterworth.

Bell, S.J., and Mengüç, B. (2002). The employee-organization relationship, organizational citizenship behaviors, and superior service quality, *Journal of Retailing*, 78, 131–46.

Bennett, R., and Robinson, S. (2003). The past, present, and future of workplace deviance research. In J. Greenberg (Ed.), Organizational behavior: *The state of the science* (2nd ed.). Mahwah, NJ: Erlbaum.

Bemardin, H.J., and Cooke, D.K. (1993). Validity of an honesty test in predicting theft among convenience store employees. *Academy of Management Journal*, 36, 1097–1108.

Berry, C. M., Ones, D. S., and Sackett, P. R. (2007). Interpersonal deviance, organizational deviance, and their common correlates: A review and meta-analysis. *Journal of Applied Psychology*, 92, 410–424.

Bommer, W.H., Grover, S.L., and Miles, E.W. (2003). Does one good turn deserve another? Coworker influences on employee citizenship. *Journal of Organizational Behavior*, 24, 181–96.

Boye, M. W., and Jones, J. W. (1997). Organizational culture and employee counterproductivity. In R. Giacalone and J. Greenberg (Eds.), *Antisocial behavior in organizations* (pp. 172–184). Thousand Oaks, CA: SAGE Publications.

Boye, M., and Slora, K. (1993). The severity and prevalence of deviant employee activity within supermarkets. *Journal of Business and Psychology*, 8, 245–253.

Brown, T. S., Jones, J. W., Terris, W., and Steffy, B. D. (1987). The impact of preemployment integrity testing on employee turnover and inventory shrinkage losses. *Journal of Business and Psychology*, 2, 136–149.

Byrne, Z. S., Stoner, J., Thompson, K. R., and Hochwarter, W. (2005). The interactive effects of conscientiousness, work effort, and psychological climate on job performance. *Journal of Vocational Behavior,* 66, 326–338.

Campbell, D. J., and Campbell, K. M. (2003). Global versus facet predictors of intention to quit: Differences in a sample of male and female Singaporean managers and non-managers. *International Journal of Human Resource Management*, 14, 1152–1177.

Chen, C.X. and Santino, T. (2008) Do internal controls mitigate employee theft in chain organizations? Retrieved July 1, 2008, from *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1004184*

Cherrington, D. J., and Cherrington, J. O. (1985). The climate of honesty in retail stores. In W. Terris (Ed.), *Employee theft: research, theory and applications* (pp. 27–39). Park Ridge, IL: London House.

Cullen, M. J., and Sackett, P. (2003). Personality and counterproductive workplace behavior. In M. A. Barrick and A. M. Ryan (Eds.), *Personality and work* (pp. 150–182). San Francisco: Jossey-Bass.

Dabney, D. (1995). Neutralization and deviance in the workplace: Theft of supplies and medicines by hospital nurses. *Deviant Behavior: An Interdisciplinary Journal*, 76, 313–331.

Dalal, R. S. (2005). A meta-analysis of the relationship between organizational citizenship behavior and counterproductive work behavior. *Journal of Applied Psychology*, 90, 1241–1255.

Dunlop, P. D., and Lee, K. (2004). Workplace deviance, organizational citizenship behavior, and business unit performance: The bad apples do spoil the whole barrel. *Journal of Organizational Behavior*, 25, 67–80.

Elovainio, M., Kivimäki, M., and Helkama, K. (2001). Organizational justice evaluations, job control, and occupational strain. *Journal of Applied Psychology*, 86, 418–424.

Elenkov, D. S., and Manev, I. M. (2005). Top management leadership and influence on innovation: Theory of sociocultural context. *Journal of Management*, 31, 381–402.

Greenberg, J. (1993). Stealing in the name of justice: Informational and interpersonal moderators of theft reactions to underpayment equity. *Organizational Behavior and Human Decision Processes*, 54, 81–103.

Greenberg, J. (1997). The STEAL motive: Managing the social determinants of employee theft. In R.A. Giacalone and J. Greenberg (Eds.), *Antisocial behavior in organizations* (pp. 85–108). Thousand Oaks, CA: SAGE Publications.

Greenberg, J. (1997). Managing the social determinants of employee theft. In R. Giacalone and J. Greenberg (Eds.), *Antisocial behavior in organizations* (pp. 85–108). Thousand Oaks, CA: SAGE Publications.

Greenberg, J. (2002a). *Managing behavior in organizations* (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

Greenberg, J., and Tomlinson, E.C. (2004). The methodological evolution of employee theft research: The DATA cycle. In R.W. Griffin and A.M. O'Leary-Kelly (Eds.), *The dark side of organizational behavior* (pp. 426–461). San Francisco: Jossey-Bass.

Griffin, R.W., O'Learly-Kelly, A., Collins, J. (1998), *Dysfunctional Behavior in Organizations*. Greenwich, CT: JAI Press.

Gross-Schaefer, A., Trigilio, J., Negus, J., and Ro, C. (2000). Ethics education in the workplace: An effective tool to combat employee theft. *Journal of Business Ethics*, 26, 89–100.

Gruys, M. L., and Sackett, P. R. (2003). Investigating the dimensionality of counterproductive work behavior. *International Journal of Selection and Assessment*, 11, 30–42.

Hanisch, K. A., and Hulin, C. L. (1991). General attitudes and organizational withdrawal: An evaluation of a causal model. *Journal of Vocational Behavior*, 39, 110–128.

Hanisch, K. A., Hulin, C. L., and Roznowski, M. (1998). The importance of individuals' repertoires of behaviors: The scientific appropriateness of studying multiple behaviors and general attitudes. *Journal of Organizational Behavior*, 19, 463–480.

Harris, L. C., and Ogbonna, E. (2002). Exploring service sabotage: The antecedents, types and consequences of frontline, deviant, anti-service behaviors. *Journal of Service Research*, 4, 163–183.

Johns, G. (1998). Aggregation or aggravation? The relative merits of a broad withdrawal construct. *Journal of Organizational Behavior*, 19, 453–462.

Jones, J.W., Slora, K.B., and Boye, M.W. (1990). Theft reduction through personnel selection: A control group design in the supermarket industry. *Journal of Business and Psychology*, 5, 275–279.

Jones, J.W., and Tenis, W. (1983). Predicting employees' theft in home improvement centers. *Psychological Reports,* 52,197–201.

Jones, J. W., and Terris, W. (1985). Screening employment applicants for attitudes towards theft: Three quasi-experimental studies. *International Journal of Management*, 2(3), 62–75.

Kacmar, M. K., Andrews, M. C., Van Rooy, D. L., Steilberg, R. C., and Cerrone, S. (2006). Sure everyone can be replaced . . . but at what cost? Turnover as a predictor of unit-level performance. *Academy of Management Journal,* 49, 133–144.

Kamp, J., and Brooks, P. (1991). Perceived organizational climate and employee counterproductivity. *Journal of Business and Psychology*, 5, 447–458.

Kim, J., Moon, J., Han, D., Tikoo, S. (2004). Perceptions of justice and employee willingness to engage in customer-oriented behavior, *Journal of Services Marketing*, 18, 267–275.

Lau, V. C. S., Au, W. T., and Ho, J. M. C. (2003). A qualitative and quantitative review of antecedents of counterproductive behavior in organizations. *Journal of Business and Psychology*, 18, 73–99.

Levine, S., and Jackson, C. (2002). Aggregated personality, climate and demographic factors as predictors of departmental shrinkage. *Journal of Business and Psychology*, 17, 287–297.

Lynam, D., Moffitt, T. E., and Stouthamer-Loeber, M. (1993). Explaining the relation between IQ and delinquency: Class, race, test motivation, school failure, or self-control? *Journal of Abnormal Psychology*, 102,187–196.

MacLean, T.L. (2001) Thick as thieves: A social embeddedness model of rule breaking in organizations. *Business & Society*, 40(2), 167–196.

Marcus, B., and Schuler, H. (2004). Antecedents of counterproductive behavior at work: A general perspective. *Journal of Applied Psychology*, 89, 647–660.

Marcus, B., Schuler, H., Quell, P., and Humpfner, G. (2002). Measuring counterproductivity: Development and initial validation of a German self-report questionnaire. *International Journal of Selection and Assessment*, 10, 18–35.

Mars, G. (1994). *Cheats at work: An anthropology of workplace crime*. London: Gower.

McFarland, L.A. and Ryan, A.M. (2006). Toward an integrated model of applicant faking behavior. *Journal of Applied Social Psychology*, 36, 4, 979–1016.

McGurn, J. (1988, March 7). Spotting the thieves who work among us. *Wall Street Journal*, A16.

Miceli, Marcia P., and Janet P. Near. (1992). *Blowing the whistle: The organizational and legal implications for companies and employees*. New York: Lexington Books.

National Computer Systems. (1998). *Employee perceptions survey*. Rosemont, IL: Author.

Niehoff, B., and Paul, R. (2000). Causes of employee theft and strategies that HR managers can use for prevention. *Human Resource Management*, 39, 51–64.

Neuman, J. H., and Baron, R. A. (1997). Aggression in the workplace. In R. A. Giacalone and J. Greenberg (Eds.), *Antisocial behavior in organizations* (pp. 37–67). Thousand Oaks, CA: SAGE Publications.

Ones, D. S., and Viswesvaran, C. (2003). Personality and counterproductive work behaviors. In A. Sagie, S. Stashevsky, and M. Koslowsky (Eds.), *Misbehavior and dysfunctional attitudes in organizations* (pp. 211–249). Hampshire, United Kingdom: Palgrave/Macmillan.

Ones, D. S., Viswesvaran, C., and Schmidt, F. L. (2003). Personality and absenteeism: A meta-analysis of integrity tests. *European Journal of Personality*, 17, S19–S38.

Palmer, E. J. (2003). An overview of the relationship between moral reasoning and offending. *Australian Psychologist*, 38, 165–174.

Parilla, P. F., Hollinger, R. C., and Clark, J. P. (1988). Organizational control of deviant behavior: The case of employee theft. *Social Science Quarterly*, 69, 261–280.

Pawlowski, R. and Hollwitz, J. (2000). Work values, cognitive strategies, and applicant reactions in a structured preemployment interview for ethical integrity. *The Journal of Business Communication*, 37, 56–76.

Robinson, S. L., and Bennett, R. J. (1995). A typology of deviant workplace behaviors: A Kulas, McInnerney, DeMuth, and Jadwinski, 401 multidimensional scaling study. *Academy of Management Journal*, 38, 555–572.

Rothschild, Joyce, and Terance D. Miethe. (1999). Whistle-blower disclosures and management retaliation: The battle to control information about organization corruption. *Work and Occupations*, 26(91), 107–128.

Rupe, R. A. (1980, March). Formula for loss prevention. *Retail Control*, 2–15.

Sackett, P. R., Burris, L. R., and Callahan, C. (1989). Integrity testing for personnel selection: An update. *Personnel Psychology*, 42, 491–529.

Sackett, P. R., and DeVore, C. J. (2001). Counterproductive behaviors at work. In N. Anderson, D. S. Ones, H. Sinangil Kepir, and C. Viswesvaran (Eds.), *Handbook of industrial, work and organizational psychology: Volume 1—Personnel psychology* (pp. 145–164). London, England: SAGE Publications.

Sackett, P. R., and Wanek, J. E. (1996). New developments in the use of measures of honesty, integrity, conscientiousness, dependability, trustworthiness and reliability for personnel selection. *Personnel Psychology*, 49, 787–829.

Sauser, W.I., Jr. (2007). Fostering an ethical culture for business: The role of HR managers. In R. R. Sims (Ed.), *Human resources management: Contemporary issues, challenges and opportunities* (pp. 253–285). Greenwich, CT: Information Age Publishing.

Schmidt, F. L. (2002). The role of general cognitive ability and job performance: Why there cannot be a debate. *Human Performance*, 15,187–211.

Schmidt, F. L., Viswesvaran, C., and Ones, D. S. (1997). Validity of integrity tests for predicting drug and alcohol abuse: A meta-analysis. In W. J. Bukoski (Ed.), *Meta-analysis of drug abuse prevention programs* (pp. 69–95). Rockville, MD: NIDA Press.

Schinnerer, J. (2003). The ROI of an effective ethics program. *Workspan*, 46(6), S2.

Shapiro, D. L., Trevino, L. K., and Victor, B. (1995). Correlates of employee theft: A multidimensional justice perspective. *International Journal of Conflict Management*, 6, 404–414.

Skarlicki, D.P., and Folger, R. (1997). Retaliation in the workplace: The roles of distributive, procedural, and interactional justice. *Journal of Applied Psychology*, 82, 434–443.

Sherman, L.W., Gottfredson, D., MacKenzie, D., Eck, J., Reuter, P., and Bushway, S. (1997). Preventing crime: *What works, what doesn't, what's promising*. College Park, MD: University of Maryland and The U.S. Department of Justice.

Slora, K. B. (1989). An empirical approach to determining employee deviance rates. *Journal of Business and Psychology* 4, 199–219.

Snider, L. (2001). Crimes Against Capital: Discovering Theft of Time. *Social Justice*, 28(3), 105–121.

Spector, P. E. (1978). Organizational frustration: A model and review of the literature. *Personnel Psychology*, 31, 815–829.

Spector, P. E. (1997). The role of frustration in antisocial behavior. In R. A. Giacalone and J. Greenberg (Eds.), *Antisocial behavior in organizations* (pp. 1–17). Thousand Oaks, CA: SAGE Publications.

Stamper, C. L., and Van Dyne, L. (2001). Work status and organizational citizenship behavior: A field study of restaurant employees. *Journal of Organizational Behavior*, 22, 517–536.

Tepper, B., Duffy, M., Hoobler, J., and Ensley, M. (2004). Moderators of the relationship between coworkers' organizational citizenship behavior and fellow employees' attitudes. *Journal of Applied Psychology,* 89, 455–465.

Tucker, J. (1989). Employee theft as social control. *Deviant Behavior*, 10, 319–334.

Wanek, J. E. (1999). Integrity and honesty testing: What do we know? How do we use it? *International Journal of Selection and Assessment,* 7, 183–195.

Weber. J., Burke. L. B., and Pentico, D. W. (2003). Why do employees steal? *Business and Society*, 42, 359–380.

Wells, J. (2005). Internal controls can give you ulcers. *The Practical Accountant*, 8, 48.

Weiss, B., and Feldman, R.S. (2006). Looking good and lying to do it: Deception as an impression management strategy in job interviews. *Journal of Applied Social Psychology*, 36(4), 1070–1086.

White, L., and Lam, L. (2000). A proposed infrastructural model for the establishment of organizational ethical systems. *Journal of Business Ethics*, 28, 35–42.

Winbush, J. C., and Dalton, D. R. (1997). Base rate for employee theft: Convergence of multiple methods. *Journal of Applied Psychology*, 82, 756–763.

Wulfson, M., (1998). Rules of the game: Do corporate codes of ethics work? *Review of Business*, 20, 1-9.

Zellars, K. L., Tepper, B. J., and Duffy, M. K. (2002). Abusive supervision and subordinates' organizational citizenship behavior. *Journal of Applied Psychology, 87,* 1068–1076.

# Appendix A: Vulnerability Checklist for Businesses

1. What is the crime risk score or crime level around the location?

2. How large is the location? What type of location is it? What are the location's most desirable assets? What market segment does it target?

3. What are the location's hours? Is it open at night? Are nearby businesses open at night and on weekends?

4. Does the location practice thorough preemployment screening and orientation?

5. Are all company employees notified and reminded of relevant company policies and procedures?

6. Are employees guided by focused, practical procedures?

7. Does the business have skilled asset protection staff?

8. Are all suspicious and known crime events recorded and analyzed for patterns?

9. Are targeted assets secured or tracked with barriers, locks, and checks and balances?

10. Is natural and CCTV surveillance leveraged on the property? Can thieves remove assets without being seen?

11. Are police notified of important incidents?

12. Does the organization have an anonymous hotline program?

13. Are point of sale and inventory transactions tracked for patterns?

14. Are employee morale and complaint levels tracked and addressed?

15. Is asset protection procedural compliance randomly audited and reconciled more than once a year?

16. Are all offenders investigated and prosecuted?

# Appendix B: Elements of a Loss Control Program

1. Screen Out Potentially Deviant Employees
    a. Conduct more than one probing interview
    b. Check three or four references for workplace patterns (hard work, compliance, teamwork)
    c. Conduct applicant credit and criminal checks
    d. Consider integrity, personality, and self-report (of past deviance) tests

1. Create a culture of honesty (reduce motives)
    a. Establish and distribute an explicit code of conduct
    b. Daily, managers set personal examples of integrity
    c. Leaders always show respect for all employees
    d. Reward hard work, compliance, and ethical behavior
    e. Seek employee input, and listen to complaints and suggestions

1. Make deviance more difficult (reduce opportunity) and riskier (increase personal risk)
    a. Restrict access to safes and other critical assets with procedures and  technology
    b. Employ check and balance control procedures
    c. Use CCTV, employee hotlines, exception reporting
    d. Audit procedural compliance and reported incidents
    e. Discipline or terminate dishonest employees
    f. Take criminal and civil action against dishonest employees

# Appendix C: Preventing Employee Dishonesty In Retail Settings

1. Never allow employees to bring their purses or packages onto the selling floor. Only clear plastic purses with essential personal items should be allowed in work areas.

2. Store high-priced and very high-loss overstock items in separate, locked, and monitored security cages for better protection. Maintain a log that documents access to the area.

3. Consider using closed-circuit television (CCTV) and/or roaming security agents in both store and distribution facilities to assist in detection and deterrence of employee theft. Because employees are often intimately aware of "hiding spots" in the store, any type of surveillance—natural or mechanical—should be thorough, covering as much of the floor as possible.

4. Offer store discounts to employees and their relatives. This can facilitate legitimate purchasing.

5. Control allocation of price guns and check prices on employee purchases to discourage unauthorized markdowns by employees and customers.

6. Authorize and verify all shipments by an employee who is not responsible for controlling inventories.

7. Require all employees to enter and leave the workplace through a designated employee entrance monitored by a security guard or management personnel.

8. Provide a room for overcoats and unusually large packages. Post a sign at this entrance warning employees that pilferage is a crime, and those caught will be prosecuted.

9. Lock roll-up receiving doors at the bottom, not at their pull chains, since employees can easily use dollies to hoist the doors open and then slide merchandise through the gap.

10. Secure all doors not used for regular customer traffic per local fire regulations and install panic alarms. Test panic doors monthly.

11. Hook doors up to a central alarm system to record openings and closings for patterns.

12. Ensure a manager observes and documents all freight deliveries made at either the distribution facility or the store.

13. Restrict access to supply areas and ensure these areas are monitored by a security guard.

14. Ensure that employees who enter the supply area are accompanied by a warehouse employee, and that they complete a sign-in sheet recording name, time of entrance and departure, and merchandise removed.

15. Keep customer returns and damaged items in a secure, monitored area.

16. Keep stockroom merchandise in neat stacks, not disorderly piles, so it is easy to spot missing items. Bad housekeeping is a quick tip-off to possible employee theft.

17. Restrict personal or unnecessary employee use of office equipment, company gas pumps, telephones, Internet, email, postage meters, and other facilities designed for company use.

18. Monitor utility, Internet use, and phone bills for patterns.

19. Escort guests and employees from other companies to their appointments.

20. Rotate employees of one department to a different department to take inventory. Ensure that inventory is supervised by a member of management.

21. Keep merchandise in neat, orderly displays. Never stack high-loss items near doors or operable windows.

22. Clearly and permanently mark company equipment with the company's name.

23. Ensure that tools and equipment are inventoried and locked up by a supervisor at the end of each workday.

24. Be suspicious of company equipment or merchandise that appears out of place. Encourage employees to report out-of-place items to management.

25. Inventory high-priced merchandise on processing lines in distribution facilities. Keep it in secured areas.

# Appendix D: Preventing Retail Fraud

1. Use shredders for all financial and other sensitive documents.

2. Have all vendors and employees sign non-disclosure forms.

3. To prevent non-registered sales, enlist customer assistance. Consider posting signs by each cash register announcing "Any customer who does not receive a sales receipt is entitled to …"

4. Designate a responsible company official, who is not on the accounting department's staff, to receive and investigate customer complaints.

5. Consider bonding key employees with access to large amounts of cash or checking accounts for theft.

6. Ensure a member of senior management supervises the accounting employee who opens and records receipt of checks, cash payments, gift cards, and money orders.

7. Ensure a manager prepares bank deposits daily. Return duplicate deposits slips, stamped "RECEIVED" by the bank, to the accounting department.

8. As well as the people who draw and sign checks, ensure that senior management approves all payments.

9. Ensure that senior management examines all invoices and supporting data before signing checks or authorizing payment. Verify the receipt and reasonable price of all merchandise. In many false purchase schemes, the embezzler will neglect to complete receiving forms or other records purporting to show receipt of merchandise.

10. Mark and record all paid invoices "CANCELED" and file them in a secure folder or area to prevent double payment. Dishonest accounting department employees have been known to make out and receive approval on duplicate checks for the same invoice. The second check may be embezzled by the employee or by an accomplice at the company issuing the invoice.

11. Periodically inspect pre-numbered checkbooks and other pre-numbered forms to ensure that checks or forms from the back or middle of the books have not been removed for use in fraudulent schemes.

# Appendix E: Ethical Practices That Can Reduce Fraud

12. Place authorized spending limits on employees and Audit company credit card use. Analyze expense reports for problems and patterns.

13. Do not permit employees responsible for making sales or assigning projects to outside suppliers to process transactions affecting their own accounts.

14. Ensure that an employee who does not draw or sign checks reconciles bank statements and canceled checks or other payments. Ensure that management examines canceled checks, transfers, and endorsements for unusual features.

1. Require competitive bidding for any service or other business.

2. Separate receiving operations from purchasing operations so buyers cannot accept short or incorrect deliveries in return for kickbacks.

3. Have an executive from outside the purchasing department review bids and randomly inspect incoming goods.

4. Require that employees, particularly those in purchasing, file monthly reports on any offers or received gifts and gratuities. Set a limit on the number and value of gifts or offers that may be accepted.

5. Insist any (approved) gifts be sent to the office, and not directly to employees' homes.

6. Inform vendors in writing each year of acceptable gift-giving practices.

7. When a supplier other than the low bidder is selected, insist that the reason be documented and sent to top management for review and approval.

8. Rotate the assignment of purchasing agents and suppliers.

9. Instruct employees to report any demands for payoffs made by customers or vendors.

10. Estimate reasonable costs for products and services, so possible kickbacks can be identified.

11. Develop policies that ensure maintenance of a professional distance between management and union officials.

12. Institute procedures that alert management when commissioned vendors make undocumented payments to employees. Commissions not aligned with recognized trade practices or made through unknown banks may indicate unethical behavior.

13. An employee or official of a company or government organization involved in a bribery, kickback, or payoff scheme may have violated any of a number of local, state, or federal laws. If you suspect one of your employees is either receiving or giving bribes or kickbacks in dealings with another non-government firm, do not confront the suspect immediately. Instead, discuss your suspicions with your company attorneys to determine what action should be taken. It is essential that your business remain within the law. Do not attempt an investigation on your own. Remember, it is not necessary for a bribe, kickback, or payoff to actually be received in order for a crime to have been committed. Under most existing legislation, the mere offering, conferring, or agreeing to confer a benefit is considered an offense.

# About the Author

**Read Hayes, PhD,** is director of the Loss Prevention Research Council, and co-director of the Loss Prevention Research Team at the University of Florida (UF). The Loss Prevention Research Council is a coalition of more than 45 leading companies that develop and measure asset protection innovation and effects. Dr. Hayes and his team are credited with changing the term "organized retail theft" to "organized retail crime" as well as coining industry terms such as "benefit denial" and "zones of influence."

Dr. Hayes began his career as a store detective in retail loss prevention in 1977.  His more than 30 years of hands-on crime and loss control experience includes working with many organizations worldwide such as Target, Home Depot, AutoZone, Macy's, Coles Meyer, Disney, P&G, Novartis, Office Depot, CVS, and Wal-Mart.

Dr. Hayes started the University of Florida's globally recognized National Retail Security Survey in 1989 with UF professors Bart Weitz and Richard Hollinger and has conducted more than 45 loss prevention field research projects. His current research focuses on such topics as offender and customer decision-making and situational deterrence, total supply chain protection, asset and key product protection, loss prevention staff selection and development, and premises violence, security, and safety.

Dr. Hayes is the author of more than 150 articles and four books, including *Retail Security & Loss Prevention* published by MacMillan. He has served as an expert resource for law firms, Fox News Network, CNN, *The Wall Street Journal*, *USA Today,* and the BBC.

He has completed numerous loss prevention courses and asset protection training programs. Dr. Hayes holds a Bachelor of Arts degree from the University of Florida and a PhD from the University of Leicester.

ASIS
INTERNATIONAL
*Advancing Security Worldwide®*

**ASIS International** (ASIS) is the largest organization for security professionals, with more than 36,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, governmental entities, and the public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine—*Security Management*—ASIS leads the way for advanced and improved security performance.

## ASIS International Foundation

The ASIS International Foundation, a 501(c)3 charitable organization, provides funding and manages endowments for a wide range of academic, strategic, and professional development activities. The purpose of the Foundation is to enhance the security profession worldwide by establishing, developing, delivering, and promoting programs that advance security through education, research, and training. Foundation scholarships ensure that those pursuing a career in security management are able to realize the highest academic achievements. Financial contributions from individuals, chapters, companies employing ASIS members, and corporations with an interest in security support the Foundation.

ASIS FOUNDATION™

1625 Prince Street
Alexandria, VA 22314-2818
USA
703-519-6200
Fax: 703-519-6299
*www.asisonline.org*