

Contents

<i>List of Figures</i>	x
<i>Preface</i>	xii
<i>Acknowledgments</i>	xiv
<i>Introduction</i>	xv
PART 1 RETAIL RISKS: PROBLEMS AND SOLUTIONS	1
Chapter 1 Employee Deviance	3
Employee error and waste	4
Merchandise theft	4
Under-ringing	4
Removal of trash	5
Controlling merchandise theft	5
Cash theft	8
Proprietary information	14
Investigating employee theft	14
Questions	16
Chapter 2 Managing Employee Honesty	17
Pre-employment screening	19
Access/procedural controls and audits	21
Store/company atmosphere	23
Questions	24
Chapter 3 Vendor Theft and Error	25
Risks	25
Questions	28
Chapter 4 Controlling Cargo Theft and Supply Chain Loss	29
Shipping	29
Staging	30
Loading	31
Transporting	31
Receiving	32
Questions	32

Chapter 5	Shoplifting	33
	Professional or convert to cash shoplifters	33
	Self-use, amateur, or opportunist shoplifters	36
	Planning for prevention	38
	People	41
	Programs and procedures	47
	Loss control policies	48
	Loss control procedures	49
	Identify and prioritize loss risks	52
	Summary	56
	Handling the shoplifter	64
	Summary	77
	Questions	79
Chapter 6	Point-of-Sale Risks	81
	Bad checks	81
	Credit card fraud	84
	Counterfeit currency	87
	Currency switch	89
	Container switch	89
	Price switch	90
	Refund fraud	90
	Quick-change schemes	91
	Questions	93
Chapter 7	Miscellaneous Risks	94
	Robbery	95
	Burglary	97
	Bomb threats	100
	Coupon fraud	103
	Crime and data loss	106
	Natural and civil disasters	107
	Civil liability and litigation	108
	Questions	112
PART II	IDENTIFYING AND PRIORTIZING RISKS	113
Chapter 8	Security Surveys	115
	Why theft, why me?	115
	Using theory to take action	117
	CPTED	117
	War of maneuver versus a war of attrition	123

	Multi-level marketing	124
	Delivery in the zones	127
	Discussion	130
	Historical data	131
	Assets to be protected	133
	Flow charting	134
	Summary	135
	Questions	136
Chapter 9	Data Analysis	137
	Possible and probable financial loss	138
	Assigning financial impact rates	139
	Probability of incident occurrence and causal probing	140
	Examining data	141
	Assigning loss incident probability rate	142
	Prioritizing risks	143
	Questions	143
PART III	DESIGNING AND IMPLEMENTING PREVENTION PROGRAMS	145
Chapter 10	Loss Prevention Program Design	147
	Basic program focus	147
	Risk control countermeasures	150
	Protection program designs	153
	The protection plan	155
	Questions	156
Chapter 11	People	157
	In-house employees	157
	Outside personnel	163
	Loss control consultants	163
	Summary	165
	Questions	165
Chapter 12	Programs	166
	Loss control policies	166
	Loss control procedures	167
	Protection programs	169
	Policy and procedure manuals	173
	Training employees	173
	Follow-up	174
	Questions	175

Chapter 13	Asset Protection Systems	176
	Access control systems	176
	Lighting	178
	Alarms	179
	Other LP systems	186
	Questions	189
Chapter 14	Selecting Protection Equipment and Services	190
	Specifications	190
	Bids	192
	Testing	193
	Negotiating the contract	194
	Questions	195
Chapter 15	Sample Protection Program	196
	Where to begin	196
	How to prepare a loss control plan	197
	Questions	201
Chapter 16	Implementing the Program	210
	Justification of the control program: making the business case	210
	Teamwork	213
PART IV	TESTING AND FOLLOW-UP OF THE LOSS CONTROL PROGRAMS	215
Chapter 17	Auditing and Follow-Up	217
	Inspections	218
	Effectiveness analysis	219
	Data collection	219
	Inspection/audit reports	219
Chapter 18	Inventories	220
	Retail method of inventory	220
	The inventory process	221
	Inventory tips	222
Chapter 19	The Future	224
	Industry trends	224
	Summary	226

Appendix 1	Sample Conflict of Interest Policy	227
Appendix 2	How-To Manual for Shoplifters	229
Appendix 3	Civil Recovery Laws	235
Appendix 4	Abbreviated Retail Security Survey (Sample)	240
Appendix 5	Sample Completed Store Audit Report	243
Appendix 6	Sample Consulting Proposal	254
Appendix 7	Recommended Control Procedures (Sample)	257
Appendix 8	Standard Operating Procedures (Sample Employee Investigation Policy)	261
Appendix 9	Training Program Checklist (Sample)	263
Appendix 10	Sample Loss Control Plan	268
Appendix 11	Sample Loss Prevention Inspection/Audit Report	273
Appendix 12	Model Civil Recovery Statute	276
Appendix 13	Model Retail Theft Statute	277
	<i>Notes</i>	281
	<i>Index</i>	283

1

Employee Deviance

Our employees can be our greatest asset, and unfortunately, our worst enemy.

Retail security studies indicate the same thing year in and year out: employees account for much if not most of store losses. This is not the case for every store or chain. But it is for many. Our employees have the best access to ALL assets. They know where cash is stashed, and they often are able to learn passwords, alarm codes, and combinations. They may even have copies of store keys. Store associates often believe they are able to accurately assess their risk of being caught if they steal. Staffers usually know about the presence or absence of security procedures and systems.

Even more importantly, employees know when alert, caring managers and staff work – as well as when naïve or apathetic associates are in charge. Dishonest employees can be motivated to steal by watching their leaders and peers break the rules; or because they feel abused or overlooked.

Employee theft and error account for the majority of retail loss. A recent survey by Ernst and Young showed that the average theft per dishonest employee amounted to \$890.¹ This figure is extremely high when compared to the average loss of \$57 per shoplifting incident. This survey indicates that loss from dishonest employees is 15 times greater than the loss caused by shoplifters.² Employees steal in a variety of ways, but the result is always the same: loss of profits and low morale. Employee theft can even lead to the loss of an entire business.

Each type of retail operation has its own unique risk areas. Drug stores carry controlled substances (prescription drugs) that must be carefully guarded. Grocers experience both employee and customer “grazing” (or eating of merchandise) on a regular basis. Fraudulent returns occur frequently in grocery operations. Also, grocery “baggers” are in an excellent position to carry merchandise to their vehicles or to those of accomplices. Cosmetics, clothes, tools auto parts, etc. are all easily worn or concealed and removed unlawfully by company employees. Employees have also been known to damage merchandise intentionally and mark it “out-of-stock.”

The methods employees use to steal company profits have been broken down into three categories – merchandise theft, cash theft, and miscellaneous business abuse. Retailers should realize many types of internal theft, such as under-ringing sales or giving away free merchandise, don't generally show up as cash shortages; instead, they impact physical inventory. This loss is often times attributed to shoplifting.

Retailers should document all reported theft and abuse incidents. These data are useful for employee management as well as to determine the most common methods of losses. Once problems are identified and prioritized, detection and prevention efforts can be focused to eliminate or control theft incidents.

Employee error and waste

Before discussing types of employee theft, it is important to address employee error and waste. Employee deviance includes malfeasance, misfeasance, and nonfeasance. Aberrant employee actions range from harmful behaviors like tardiness and chronic absence to errors resulting from inattention to detail to interpersonal behaviors like rudeness, threats, and attacks to theft and fraud. When employees are poorly trained or motivated, costly errors and actions can result. However, the enforcement of specific store policies can reduce employee error and waste. At the vendor delivery point, ensure piece counts are carefully made to verify the quantity of incoming merchandise. Ensure that merchandise is properly priced and distributed. Also, motivate register clerks to remain alert; this will minimize the mis-ringing of items. The best defense against “paperwork” shrink due to employee error and waste is thorough effective training, supervision, and discipline. Retail management should not tolerate an ill-conceived or poorly executed training program.

Merchandise theft

There are many types of merchandise theft-store and distribution employees may conceal, take, or wear company merchandise home on a regular basis. They may also hand off merchandise to friends or family members, a practice called *sweethearting* or *sliding*. In malls or shopping centers, employees are known to trade with clerks from adjacent stores or warehouses; allowing them to take merchandise in exchange for the same privilege in their store. A discussion of every method of merchandise theft is beyond the scope of this book. However, some common theft methods are discussed in the following paragraphs.

Under-ringing

When an employee under rings a purchase, he or she allows an accomplice to purchase something for a reduced price. \$10 items, for example, are rung up as 10 cents. Managers should be alert to any clerk who acts too familiar

with a customer, while quickly glancing around. A computer-generated or hand-written report on price variances is an excellent tool for detecting this problem. This report should indicate the current price of a purchased item versus the priced paid for the item. If a pattern of this type of transaction is evident, it may indicate system error, poor training, poor employee aptitude or attitude, or theft. Managers and loss prevention (LP) specialists should also note if registers equipped with price “wands” or bar code readers are being bypassed and items are being hand-keyed into the register, as this may also indicate under-ringing of merchandise.

Removal of trash

Another common method employees use to steal merchandise involves placing items in plastic garbage bags or boxes and removing them from the store. This practice is easily remedied, as clear trash bags will reveal any illegitimate contents. However, management should supervise all trash removal. Ensure the employee tears open the bag and allows the contents to fall into the dumpster. Many store managers have been surprised by the sight of jogging suits, DVDs, auto parts, etc. falling from trash bags. Also, never give employees store keys or alarm codes to remove trash or boxes on their own.

Controlling merchandise theft

Consider placing disposable or one-way Electronic Article Surveillance (EAS) tags in certain items to deter theft. EAS tags can deter some offenders, particularly if they are hidden in pockets or under the removable soles of shoes, for example. Hidden EAS tags may also function in warehouse situations.

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.

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

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.

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

Control allocation of price guns and check prices on employee purchases to discourage the unauthorized marking down of items by employees and customers. Check employee purchases.

This procedure is simple and requires all purchases made by an employee be kept in a central location. These checks should be done on a random basis. Record each purchase made by an employee or family member.

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

Require all employees to enter and leave the work place through a designated employee entrance that is monitored by a security guard or management personnel.

Provide a coatroom 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.

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

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

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

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

Ensure 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.

Keep customer returns and damaged items in a secure area.

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.

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

Escort guests and employees of other companies to their appointments.

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

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

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

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

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

Ensure that security or management personnel periodically inspect rubbish piles and garbage containers for concealed items.

Inventory high-priced merchandise on processing lines in distribution facilities and keep it in secured areas.

Assure employees that the identity of anyone who reports dishonesty on the part of other employees will be held in confidence.

Install telephone hotlines or offer rewards for theft information.

Establish a toll-free, 24-hour hotline to better facilitate company employees reporting theft, fraud, substance abuse, or sexual harassment in the workplace. Companies may use an outside service or set up an in-house hotline operation. Management should be aware, however, that many honest employees may be unwilling to "snitch."

Peer Reporting

Many experts estimate that 40% to 50% of retail losses are attributable to employee theft. As a result, loss prevention efforts have begun to focus on ways of reducing theft by employees. Many different techniques, such as electronic monitoring, education programs and fraud assessment questioning, are being used to reduce employee theft.

One of the most effective techniques is to have employees monitor and report suspicious, illegal or unethical behavior of *other employees*. Employees are more likely to be aware of activities that might otherwise be difficult to detect, and employees can detect dishonest or suspicious activities by other employees more quickly than financial audits or exit interviews.

Employee monitoring may be among the most cost-effective ways of reducing shrinkage. Techniques may include telephone hotlines, incentive and award systems, and the creation of an environment that expects employees to monitor and report the illegal or suspicious activities of other employees. Employees are more likely to report on others when in an environment where theft is clearly not an acceptable behavior.

Successful reporting programs, therefore, must provide the mechanisms, incentives, and environment to encourage employees to report theft or inappropriate behaviors by other employees.

Cash theft

Unfortunately, cash theft by dishonest employees is a common problem. Retail firms are particularly vulnerable to cash theft, since many employees have access to cash registers and counting rooms, and routinely make cash deposits.

When customers purchase items with cash, that money goes into a cash register. Therefore, the first place to look for cash theft is at the point of sale. Some employees' void legitimate sales transactions (and pocket the cash) to ensure that the register isn't "short" money at the end of the day. Clerks will also take cash from a customer and fail to ring up the sale. In many cases, the dishonest employee keeps a written record of the amount of cash they have accumulated and sets that money to the side of the cash drawer. If the employee is "spooked" or unable to retrieve this cash from the register, a cash overage results. This also occurs when an employee fails to subtract sales tax or odd change collected.

Refund fraud

In today's hassle-free customer service environment, retailers are inevitably vulnerable to refund fraud. Customers expect to be able to exchange or return merchandise with relative ease, but nefarious employees can easily take advantage of lax refund policies. The challenge, then, is to keep legitimate customers happy while also preventing fraud. Some refund policies can provide a happy medium between "no refunds" and "anything goes." When employees decide they need cash immediately and don't want to "till-tap" or void a transaction, the easiest thing to do is pull out a refund slip, or use the POS system, pick a name and address from a phone book, and using that identity, record the amount of cash they desire as refund, on a slip they then sign and date. The slip is then substituted for cash.

Some refund fraud countermeasures include numbering refund slips and logging them out as needed. Therefore, a member of management should always authorize refunds greater than \$100. Customers should sign the refund slip, along with the issuing clerk and the employee who returns the merchandise to the sales floor. Management personnel should randomly call customers who return merchandise and inquire of the transaction was handled to their satisfaction. This is not only a positive customer service strategy, but may expose a dishonest employee if a customer claims to have never been in the store. On the other hand, managers should always pass along positive customer comments to store employees – preferably in a group meeting. This serves to recognize the courteous employee, while at the same time reinforcing to staff that management *is* checking refunds and returns.

Layaway fraud

Many stores have layaway plans; this is another customer service tactic that dishonest employees can steal from. 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 fraudulently forfeiting a layaway deposit, management should authorize all deposit transactions. Similarly, a manager's authorization should also be required to prevent fraudulent layaway cancellations or payment voids.

Embezzlement and employee fraud

Retail embezzlement can occur at any level of the organization. The term "embezzle" refers to the stealing of company money by someone in a position of trust. 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, which will be further discussed in Chapter 4.

Bank deposit rolling

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. This type of crime is not very common. It can easily be prevented by having two separate employees verify each day's deposit on a rotating basis.

Check kiting

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 accomplice. Once a check from the company is deposited into an employee account, the employee makes a withdrawal of cash in that amount from their account. Before the original check clears the company account, the employee deposits a check from their account into the company's to cover the original account. This cycle continues until the kite "breaks" when either the company or one of the banks refuses to honor the checks.

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 member of management should be verify and approve all bank deposits.

Payroll fraud

Payroll fraud usually occurs when an employee (with the access and authority to add employees to payroll roster) adds fictitious names to the rosters.

Paychecks are then issued either to the dishonest employee or an accomplice. To avoid this, retailers should divide payroll functions between at least three people who prepare, verify, and distribute the payroll.

Travel and expense account fraud

With today's employees traveling more and more for business, expense reports and accounts have become prime targets for fraud. Employees typically list personal expenses such as meals and telephone calls on reports, and then submit them 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.

Controlling cash theft

Other measures retailers can use to control theft of cash by employees are:

Ensure that names on payroll rosters are authorized, in writing, by a designated company official.

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

Hire "outside shoppers", and provide them with funds to make purchases in the store. They can provide valuable information on whether salespeople are courteous, proficient, and properly reporting sales.

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

Bond key employees for theft.

Establish a good audit program that establishes and maintains a working climate of accountability in which accurate records are kept and regularly audited. (Audit programs are discussed in greater detail later in the book.)

The Small Business Association (SBA) also recommends the following procedures:

Carefully check prospective employees' backgrounds, particularly those to be given fiduciary responsibilities. This check should include oral and written contacts with previous employers, credit bureaus, and personal references. Make sure that an employee who will handle funds is adequately bonded.

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

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

Ensure that senior management (as well as the person who draws or signs the checks) approves all payments.

Ensure senior management examines all invoices and supporting data before signing checks. 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.

Mark all paid invoices as "CANCELED" and file them in a secure 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.

Periodically inspect prenumbered checkbooks and other prenumbered forms to ensure that checks of forms from the back of middle of the books have not been removed for use in a fraudulent scheme. Place authorized spending limits on employees.

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

Ensure that an employee who does not draw or sign checks reconciles bank statements and canceled checks. Ensure management examines canceled checks and endorsements for unusual features (see Chapter 7).

Payroll should be prepared by one person, verified by another, and distributed by others not involved with the payroll preparation or time slip approval.

Miscellaneous business abuse

The third major category of internal theft risk is *miscellaneous*. This includes abuses such as unethical conduct, time theft, and drug abuse.

In the U.S., business ethics are under increased scrutiny as more well-known government and private enterprises face criminal indictment. In a retail business, most key employees are in a position to accept a bribe or kick back from a product or service vendor. Merchandise buyers, purchasing agents, 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 a position to recommend or authorize agreements with outside vendors.

Retailers can reduce their vulnerability to this type of crime by taking some the following actions:

Require competitive bidding for business.

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

Ensure an executive from outside the purchasing department reviews bids and inspects incoming goods.

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

Insist that gifts be sent to the office, not to the employees' homes.

Inform vendors of acceptable gift-giving practices.

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.

Rotate the assignment of purchasing agents and suppliers.

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

Make estimates of reasonable costs for products and services, so that possible kickback costs can be identified.

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

Institute procedures that alert management when payments of commissions by vendors to employees are not documented by the usual paperwork. Commissions not in line with recognized trade practices or made through banks not usually used, may indicate unethical behavior.

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 that 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 undertaken. It is essential that your business stay within the law. Therefore, do not attempt an investigation on your own. Remember, it is not necessary that a bribe, kickback, or payoff 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.

Another form of miscellaneous abuse is time theft. 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 good morale all help control time abuse.

In an effort to make company employees or associates feel like they are a part of their company, many retailers offer employee discounts on store merchandise. The discount is usually averages around 10% on low-margin items and 20% on others. Employee discount programs are a boost to employee morale. The company's discount policy should be in written form and monitored by store managers. Unfortunately, discount policy violations are now the most common form of internal theft. Abuse often involves extending the employee discount to individuals not authorized to receive it. Some dishonest employees purchase items with their discount and have an accomplice return the items for the higher regular price.

Stores that have discount programs report that they average between .25% and 1.10% of gross annual sales in employee purchases. This percentage varies with the size of the company and the type of merchandise sold. If a chain has a store that greatly exceeds or doesn't meet the established, average percentage of gross sales in employee purchases, employees may be abusing the privilege or just outright stealing the merchandise.

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" company assets for personal endeavors. Management should inventory and permanently mark valuable items, and secure sensitive areas to help control this type of loss.

Another significant method of employee theft involves filing false workers' compensation claims. This practice may be replacing unemployment claims as a desirable source of income. Management should investigate all workmen's compensation claims to determine if abuse is occurring.

Unsupervised work crews, laid-off employees, and others such as disgruntled union members may inflict damage on the retailer in the form of vandalism or sabotage. Distribution of company assets and work stoppage are examples of this type of risk. Supervisors should keep the lines of communication open in an effort to determine if morale problems exist. They should also debrief terminated or laid-off employees prior to departure and deny them access to sensitive areas.

Every business is vulnerable to theft via cleaning crews. Therefore, it is essential to supervise in-house or contract cleaning personnel. Random checks of tool boxes, cans of wax, vacuum cleaner bags, and trash is a must.

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 cause accidents and increased theft activity in the workplace. Employers should screen applicants to keep individuals with untreated addictive or criminal tendencies from entering the company workforce. Train supervisors to detect and refer problem employees to Employee Assistance Programs (EAP's). Retailers face liability if dependent employees go untreated and severe losses, injuries, or even death occurs. Consultation with government or private experts regarding an effective EAP is recommended. Some retail businesses are placing undercover agents in their operation to discover the source of suspected theft or substance abuse activity.

Proprietary information

All retail 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. Retailers must ensure that confidential information is carefully guarded. There is a difference in the civil and criminal rights afforded to retailers depending on the type of information being protected. Trade secrets may be subject to greater protection under federal law if it can benefit and that the company makes reasonable efforts to maintain its secrecy. An employees can seriously undermine a company if he or she divulges trade secrets – either intentionally or not. A minimal proprietary information security plan should include the following:

1. Restrict non-employee access to areas containing confidential information.
2. Use warning signs and instructions to alert employees to the sensitivity of certain things or places.
3. Inform employees and visitors of the confidentiality of certain areas or information.
4. Store sensitive documents separately in containers for which special security precautions are taken.
5. Impose area controls within a facility among different classes of employees with respect to certain information or operations.
6. Instruct employees and suppliers 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, but some of the most common are: spot audits, follow-up investigations

resulting from inventory shortages, gross margin problems, price variances, and when an accomplice or witness tips off management.

LP personnel or trained consultants should vigorously investigate all accusations and indications of theft activity. The goals of any investigation are to substantiate the accusation or clear the suspect, discover the extent of the damage or loss and employee involvement, recover lost assets (see Figure 1.1 for a sample restitution agreement), and determine the circumstances that initially led to the incident. A retail investigator should be a neutral, third party and enter the investigation with an open mind. The normal investigative routine is to first gather evidence of wrongdoing through review of documentation and/or surveillance activities. Next, the investigator should create a list of suspects, narrow it down, and conduct preliminary interviews. Once the theft is discovered, the investigator should determine whether enough

RESTITUTION AGREEMENT AND PROMISSORY NOTE	
Non-Interest Bearing	
To Whom It May Concern:	
I, _____, do hereby promise to repay the amount of: _____ (\$ _____).	
This amount of money is the amount which I am responsible for taking from my employer _____ from _____ to _____.	
I, _____, agree to repay the above amount (\$ _____) as follows:	
<ol style="list-style-type: none"> 1. Equal monthly payment of \$ _____ for _____ months. 2. Lump sum repayment of \$ _____ on or before _____. 3. Final payment of \$ _____ due on or before _____. 	
The above agreement is voluntarily signed by:	
NAME (PRINT) _____	
ADDRESS _____	
CITY _____ STATE _____	
DATE SIGNED _____	
D.O.B. _____ PHONE () _____	
SIGNED _____	DATE _____
WITNESS SIGNATURE _____	DATE _____

Figure 1.1 Sample restitution agreement and promissory note

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 dropped. Investigators should work closely with Human Resources, Personnel, and store operations at this point; the resulting cooperation and interdisciplinary expertise will surely benefit the investigation. It is also important to remember that investigations handled without professionalism or confidentiality can face serious liabilities, so all implicated employees must be presumed innocent until proven otherwise. Thorough investigations should be conducted in an environment that stresses employee rights. Investigators should keep in mind that union activity is not to be investigated by the retailer. Only violations of the law or company policy are to be investigated.

Questions

What are three ways you can contribute to the prevention of employee merchandise theft?

How can a retailer affect employee behavior so as to deter theft?

What are some strategies for limiting the risk of proprietary information theft?

What is embezzlement?

If you suspect someone is giving or receiving kickbacks or bribes, what should you do?

Index

- Access controls 176–7
- Accidents, liability for customer and employee 108–9
- Accumulated delay time 131
- Alarms/sensors
 - area/space protection sensors 179–80
 - follow-up on 182–3
 - merchandise 183
 - object/point protection sensors 180
 - placement of 181–2
 - purpose of 179
 - robbery duress 183
 - selection of 181
 - sensor defeat techniques 182
- Alcohol abuse 14
- American Trucking Association 29
- Application screening 19
- Apprehending shoplifters 70–2
- Apprehension program 206
- Area/space protection sensors 179–80
- Audit programs
 - controlling cash theft and 10, 22–3
 - data collected from 219
 - description of 205–6
 - follow-up and 217–9
 - implementation of 217–8
 - as part of a deterrence program 172
 - purpose of 217–9
- Audit reports 219
 - sample of loss prevention 273–5
 - sample of store 243–53
- Awareness programs
 - employee 52, 171, 204–5
 - public 171
- Background checks 20
- Bank deposit rolling 9
- Bar coding
 - benefits of 151, 187
 - price switching and 63
 - shoplifting and 39
- Bids, securing 192–3
- Bomb threats 100–3
- Break-in burglaries 98
- Bribery 12
- Burglars, types of 98
- Burglary
 - prevention 98–100
 - types of 97
- Cargo theft, controlling
 - loading and 31
 - receiving and 32
 - shipping and 29–30
 - staging and 30–1
 - transporting and 31–2
- Cash controls 22–3, 167–8
- Cash theft 4
 - embezzlement and employee fraud 9–10
 - how to control 10–11
 - how to detect 8
 - layaway fraud 8–9
 - refund fraud 8
- CCTV, *see* Closed-circuit television
- Charge-backs 26
- Check(s) 84
 - bad 81–3
 - clearing services 82
 - kiting 9
 - traveler's 82
- Civil action
 - company policy on 23
 - programs 172
 - shoplifting and 77
 - theft and 237–8
- Civil disasters 107–8
- Civil recovery laws 235–8
- Civil recovery statute, model 276
- Cleaning crews, theft by 13
- Closed-circuit television (CCTV) 5, 61–2
 - description of 185–6
 - labor requirements of 151
 - robbery and 96
- Colored signs, use of 187

- Company policies
 - and procedure manuals 173
 - regarding theft 23
 - security surveys and review of 134-5
 - updating 174
- Computer crime and data loss 106-7
- Computerized time systems 188
- Conflict of Interest Policy,
 - sample of 227-8
- Consultants, loss control 163-5
- Consulting proposal, sample 254-6
- Container switch 89
- Cost(s)
 - avoidance 211
 - direct 138
 - indirect 138-9
 - insurance 139
 - justification of loss prevention program 211
 - lost income, formula for 139
 - permanent replacement 139
 - related 139
 - of shoplifting 4, 38
 - temporary replacement 139
- Counterfeit currency 87-8, 188
- Coupon fraud 103, 104-6
- Credit card fraud 84-7
- Currency
 - classes and colors of treasury seal and serial number 87
 - counterfeit 87-8, 188
 - raised 89
 - switch 89
- Customer convenience and perception,
 - risk control and 151
- Defense in depth 131, 155
- Delivery control procedures 27
- Delivery persons, dealing with 26
- Detachers 232-3
- Detaining shoplifters 69, 72-3, 76-7
 - liability and 109-10
- Detection loss prevention
 - program 171-2
- Detectives/agents, loss control
 - and 159-60
 - auditing programs 172
 - exception reports 172
 - store agent patrol 172
- Deterrence loss prevention
 - programs 169
 - control procedures 171
 - detection programs 171
 - employee awareness 171
 - new store/site selection 169
 - public awareness campaigns 171
 - store environment design 170-1
- Director/vice president of security or
 - loss control 157-8
- Displays, secure merchandise 51, 186-7
- Dressing room control
 - role of fitting room attendants 160
 - shoplifting and 58, 229-30
- Drive-off burglaries 97
- Drug abuse 14, 225
- Education verification 19
- Electronic Article Surveillance (EAS)
 - description of 183-5
 - labor requirements and 151
 - tags 5, 21, 51
- Embezzlement and employee
 - fraud 9-10
- Employee(s)
 - awareness programs 52, 171, 204-5
 - benefits of offering discounts to 5, 13
 - direction and discipline 175
 - error and waste, how to control 4
 - investigation policy 261-2
 - rewards and recognition of 174-5
- Employee Assistance Programs (EAPs) 14
- Employees, loss control and role of
 - detectives/agents 159-60
 - director/vice president 157-8
 - fitting room attendants or store monitors 160
 - investigators/auditors 159
 - line managers 159
 - regional/district operations managers 162
 - senior managers 162
 - shortage control committees 158
 - store/distribution center 163
 - store manages 162-3
 - uniformed guards 160, 165
 - see also* Security personnel
- Employee theft
 - cash theft 3-4, 8-11

- Employee theft (*Contd.*)
- categories of 4
 - company attitudes toward 23
 - detection of 14-6
 - future for 225
 - how to control 19-24
 - merchandise theft 4, 5-7
 - miscellaneous business abuse 4, 11-4
 - shoplifting versus 3
 - statistics on 3
 - types of risk areas 3
- Employee thieves, psychological
- predictors of 17-9
- Employment/education verification 19
- Environmental design and physical layout 170-1
- Ernst and Young 3
- Exception reports 172
- Expense account fraud 10
- False arrest and imprisonment 109-11
- Financial loss
- assigning financial impact rates 139-40
 - possible and probable 138-9
- Fitting/dressing room control
- role of fitting room attendants 160
 - shoplifting and 58, 229-30
- Flow charts, use of 134-5
- Freight charges 25-6
- Goals, loss control department 202
- Graphoanalysis 20
- Guards, loss control and
- uniformed 160, 165
- Handwriting analysis 20
- Identification dye sprays and marking pens 188
- Incident calendars 141
- Information security 131
- Inspection programs 218-9
- Inspection reports, sample of loss prevention 273-5
- Insurance 57, 172
- Interdepartmental meetings 208
- Interviews, integrity 19-20
- Inventories
- how to do physical 221-2
 - retail method of 220-1
 - tips for conducting 222-3
- Investigators/auditors,
- loss control and 159, 164
- Jones, J.W. 17
- Kickbacks 12
- Labor requirements,
- risk control and 151
- Lapping 9
- Layaway fraud 8-9
- Liability and litigation
- customer and employee accidents 108-9
 - false arrest and imprisonment 109-10
 - inadequate security lawsuits 110-1
 - wrongful discharge suits 110
- Lighting 178-9, 187
- Line managers, loss control and 159
- Loading, cargo theft and 31
- Locks 177-8
- Loss control
- apprehension and 206
 - area analysis and 206
 - auditing and 205-6, 217-9
 - awareness 204-5
 - department goals 202
 - follow-up to 174-5, 217-9
 - individual departmental tasks and 207
 - interdepartmental tasks and 207
 - policies 166-7
 - policy and procedure manuals 173
 - procedural controls 167-8
 - sample of procedural controls 259-60
 - sample plan for 268-72
 - situational or informational procedures 168-9
 - training objectives 203
 - training of employees 173-4
 - training schedule 209
 - trends in 224-6
- Loss prevention program,
- implementation of cost justification 211
 - importance of teamwork 213
 - selling to senior management 211-2

- Loss prevention program design
 - basic program focus 147–9
 - central department
 - organization and 160–1
 - cost-effectiveness and 150
 - customer convenience and
 - perception and 151
 - defense in depth or layering and 155
 - detection 171–2
 - deterrence 169–71
 - developing a list of tasks, time lines, and assets 196–7
 - guarantees and 152
 - labor requirements and 151
 - levels of security and 154–5
 - people and 157–65
 - program manageability and 151–2
 - protection program designs 153–6
 - recovery 172–3
 - redundancy and 150
 - risk control countermeasures 150–3
 - steps for creating 197–201
 - teamwork and 150–1
 - threat analysis and 152–3
 - time sensitivity of 151
 - types of security and 153–4
- Management, selling the protection program to senior 211–2
- Managers and loss control, role of
 - regional/district operations 162
 - senior 162
 - store 162
- Marein, R. 170
- Merchandise
 - alarms 183
 - controls 21–2, 49, 168
- Merchandise displays
 - secure systems 186–7
 - shoplifting and 51
- Merchandise theft 4
 - how to control 5–7
 - removal of trash 5
 - sweethearting 4
 - underringing 4–5
- Mirrors, use of 188
- Miscellaneous business abuse 4, 11–4
- Natural disasters 107–8
- Object/point protection sensors 180
- Observation towers 188
- Operating procedures, sample of standard 261–2
- Paper hangers 82
- Paper shredders 187
- Paperwork controls 168, 225
- Payoff schemes 12
- Payroll fraud 9–10
- Personnel, loss control and outside, *see* Security personnel
- Personnel security 153–4, 156
- Physical barriers 177
- Physical layout,
 - loss control and 50–1, 170
- Plot maps 141
- Point-of-sale risks
 - bad checks 81–4
 - container switch 89
 - counterfeit currency 87–8
 - credit card fraud 84–7
 - currency switch 89
 - price switch 90
 - quick-change schemes 91–2
 - refund fraud 90–1
- Policy and procedure manuals 173
- Possible financial loss 138–9
- Pre-employment screening 19–20
- Price look-up 90
- Price switch 90
- Price variances, importance of
 - reports for 5
- Private investigators,
 - loss control and 164
- Probable financial loss 138–9
- Proprietary information 14
- Prosecution, company policy on 23
- Protection equipment,
 - see* Security systems/hardware
- Protection program designs,
 - see* Loss prevention program design
- Public awareness campaigns 171
- Quick-change schemes 91–2
- Raised currency 89
- Receivers, checking 25–6
- Receiving, cargo theft and 32
- Recovery of assets 211

- Recovery programs 172–3
- Reference checks 19
- Refund fraud 8, 90–1
- Retail theft statute, model 277–80
- Return on Investment (ROI) 211
- Returns
 - types of store policies 90–1
 - vendors and 26
- Rewards and recognition,
 - employee 174–5
- Risk control countermeasures
 - cost-effectiveness 150
 - customer convenience and perceptions 151
 - labor requirements 151
 - program manageability and redundancy 150 151–2
 - teamwork 150–1
 - threat analysis and time sensitivity of 151
- Risk management techniques
 - decision matrix 147–8
 - risk acceptance 149
 - risk avoidance 148
 - risk reduction 148
 - risk spreading 148–9
 - risk transfer 149
- Risk, prioritizing 137, 143
 - by assigning financial impact rates 139–40
 - by assigning loss incident probability rate 142
 - determining probability of incident occurrence and 140–1
 - examination of security data and 141–2
 - by possible and probable financial loss 138–9
- Robbers, types of 95–6
- Robbery
 - definition of 95
 - duress alarms 183
 - how to act during a 96–7
 - prevention methods 96
 - what to do after 97
- Safes 178
- Safety controls 168
- Security
 - in depth layering 155, 156
 - levels of 154–5
 - types of 153–4
- Security lawsuits, inadequate 110–1
- Security personnel
 - expert witnesses 164
 - featured speakers/trainers 164
 - loss control consultants 163–5
 - private investigators 164
 - shopping services and plainclothes agents 164–5, 172
 - uniformed security guards 160, 165
- Security surveys
 - accumulated delay time 131
 - collection of historical data 131–3
 - defense in depth 131, 155
 - definition of 130–1
 - identifying assets to be protected 133–4
 - methods of collecting data for 131
 - review of company policies and procedures 134–5
 - sample of abbreviated retail 240–2
 - use of flow charts 134–5
- Security systems/hardware
 - access controls 176–7
 - alarms/sensors 179–83
 - bar coding 187
 - closed-circuit television 5, 61–2, 96, 151, 185–6
 - colored signs 187
 - computerized time systems 188
 - electronic article surveillance 5, 21, 51, 151, 183–5
 - identification dye sprays and marking pens 188
 - integrated 189
 - lighting 178–9, 187
 - locks 177–8
 - merchandise displays and tie-downs 186–7
 - paper shredders 187
 - physical barriers 177
 - safes 178
 - subliminal messaging systems 134, 270
 - surveillance aids 188
 - two-way radios 188–9
 - visual deterrents 187

- Security systems/hardware, selecting
 - determining specifications 190–2
 - installation and follow-up 195
 - negotiating the contract 194–5
 - securing bids 192–3
 - testing of items before purchasing 193
- Sensors, *see* Alarms/sensors
- Shipping, cargo theft and 29–30
- Shoplifters
 - apprehending 70, 71
 - detaining 72–3, 76–7
 - how to detect 66–7
 - how-to manual for 229–34
 - methods of approaching 70, 71
 - opportunist/amateur 36–7
 - professional 33, 35
 - steps to follow prior to detaining 70–2
 - true professional 35
- Shoplifting
 - civil action and 77
 - closed-circuit television and 5, 61–2
 - costs of 4, 38
 - electronic article surveillance tags
 - and 5, 21, 51
 - employee awareness programs and 52
 - employee theft versus 3
 - fitting/dressing room control for 58
 - future for 225–6
 - how to prevent 38–41
 - manual 229–34
 - merchandise display and 51
 - methods 36
 - plainclothes agents and 46
- Shortage control committees 158
- Short-packaging 31
- Site selection, loss control and 169
- Small Business Administration (SBA) 10
- Smash-and-grab burglaries 97–8
- Staging process, cargo theft and 30–1
- Stay-behind burglaries 97
- Store/distribution center employees,
 - loss control and 163
- Subliminal messaging systems 134, 270
- Supplies, pilferage of 13
- Surveillance aids 188
- Sweethearting 4
- Tax write-offs 173
- Teamwork
 - implementation of loss prevention
 - program and importance of 213
 - loss prevention program design
 - and 150–1
- Termination, company policy on 23
- Terris, W. 17
- Testing
 - for honesty 20
 - of security items before
 - purchasing 193
- Threat analysis, loss prevention
 - program design and 152–3
- Tie-downs 187–8
- Time sensitivity, loss prevention
 - program design and 151
- Time systems, computerized 188
- Time theft 13
- Training organizations, list of 268
- Training programs 23
 - checklist for 263–7
 - description of 173–4
 - objectives for 203
 - for plainclothes agents 46
 - preparing for 200–1
 - schedule for 209
- Transporting, cargo theft and 31–2
- Trash removal, theft and 5–7
- Travel account fraud 10
- Traveler's checks 82
- Two-way radios 188–9
- Underringing 4
- Unethical conduct 11–2
- Uniformed security guards 160, 165
- U.S. Congress, Committee on Bank
 - and Finance of 84
- Universal product code (UPC),
 - see* Bar coding
- Vendor theft and error,
 - risks of 25–8
- Visual deterrents 187
- Witnesses, use of expert 164
- Worker's compensation claims,
 - filing false 13
- Wrongful discharge suits 110