CURTAILING CRIME -- INSIDE AND OUT

Crime Prevention Series

Contributors to the text were Saul D. Aster, President, Management Safeguards, Inc., New York, NY; S.J. Curtis, Management Consultant, Dayton, OH; Leonard Kolodny, Manager, Retail Bureau, Metropolitan Washington Board of Trade, Washington, DC; Christopher J. Moran, CPA, Partner, A.M. Pullen and Company, Greensboro, NC; and Addison H. Verrill, Dale System, Inc., Garden City, NY.

TABLE OF CONTENTS

INTRODUCTION

This publication outlines some positive steps to help curb crime. These include safeguards against employee dishonesty, ways to control shoplifting, means to outwit those who pass bad checks and means to prevent burglaries and robberies.

SAFEGUARDS AGAINST EMPLOYEE DISHONESTY

Loss by theft in retail establishments varies by the type of operation and the efficiency of management. Losses range, for example, from 1.3 percent of sales for a well-managed

department store to about 7 percent for a loosely controlled operation. According to one estimate, dishonest employees account for about two-thirds of retail theft and shoplifting for the remaining third.

Even though you cannot eliminate stealing entirely, you can take steps to minimize it. The key lies in the proper mix of the right controls.

The best safeguard against employee theft is the worker whose integrity is beyond question. Too many retailers take integrity for granted. A store owner should take every precaution to ensure that the people hired are honest, and then, maintain the kind of store climate that will encourage them to stay honest.

Screen Applicants

Just like a book, a job applicant can't be judged by outward appearance alone. Appearance, experience and personality may all be in the applicant's favor, but he or she may still be a thief or other high security risk. Remember that the person you easily pick may just be looking for easy pickings.

In hiring, apply strict screening standards and, no matter how urgently you may need additional personnel, do not compromise those standards. Screen applicants through reference checks, credit checks, psychological tests, polygraph lie-detector tests and personal character examinations. Be sure to adhere to the law in performing these checks.

Observe New Employees

Lack of knowledge about the store's routine usually restricts new employees' stealing to what they can slip from the cash register or conceal on their persons. You can detect both by closely watching daily receipts and scrutinizing new employees until you are satisfied that you can trust them.

Establish a Positive Atmosphere

Another important step to eliminating employee dishonesty is to set a tone or atmosphere that encourages honesty in your store. Expect excellence from your employees, and live up to that standard yourself. People tend to copy individuals who set such standards and require that they be met. If an employee sees a supervisor in even a minor dishonest act, he or she might be encouraged in the same direction. When you set rules, be sure they apply to everyone.

Preserving the dignity of your employees is essential if you expect them to respect you and the store. Treat employees with courtesy and consideration. Show an interest in them as individuals. Then back up that interest -- to mention an example or two -- by keeping rest rooms and other areas clean and attractive and by providing fresh uniforms, if applicable. Respecting employees may not reform the hardcore thief but it will keep many others from straying.

Provide Incentives for Honest Employees

A third step in upgrading personnel is to enable employees to live up to your expectations. The following practices can help:

- *Make certain each person is matched to his or her job*. Setting unrealistic goals for employees is an invitation to them to cheat. If your goals are unrealistic, employees may think they must either cheat or admit failure and risk losing their jobs. Lying and cheating, even on a small scale, are just a step away from theft.

- *Set reasonable rules and enforce them rigidly*. Loosely administered rules are more harmful than no rules at all.

- *Set clear lines of authority and responsibility*. Each employee needs a yardstick by which to measure his or her progress and improve performance. To fill this basic need, spell out duties, preferably in writing. When employees do not know who does what, there will be error, waste and the kind of indifferent performance that breeds dishonesty.

- *Establish a climate of accountability*. Employees should know their jobs and feel trusted. But they should also realize that they are accountable for their actions. To some people, management indifference is a license to steal.

- *Provide the necessary resources for success*. As buyers, salespeople or stock clerks, nothing is more frustrating to employees than to see their goals blocked by circumstances beyond their control. To perform well, an employee needs the proper tools, the right information and guidance when it is required. Denying such support but still expecting employees to produce is a sure way to weaken morale.

- *Be fair in rewarding performance*. The top-producing salesperson who receives the same treatment as the mediocre employee is apt to become resentful. Individuals who make a worthwhile contribution are entitled to, and expect, a fair reward. Honest recognition of merit by the owner-manager encourages more honest effort on the part of the employee.

- *Remove the temptation to steal*. One organization of counter service restaurants is noted for its good employee relations. It treats people fairly and displays faith in their integrity and ability. But it also provides uniforms without pockets. Remove the opportunity to steal and half the battle is won. There is no substitute for rigid, well-implemented preventive measures.

- *Train employees to control stock shortages*. Train employees in ways to eliminate stock shortage and shrinkage. One small retailer, for example, trains employees to record items, such as floor cleaner, that they take out of stock for use in the store. It is important to adopt a zero shortage attitude. Even if you feel that a reasonable write-off due to theft is all right, keep it a secret and hammer away at shortage

control, even when losses diminish.

! *Remain alert*. Never stop letting your people know that you are always aware and concerned. This point must be driven home again and again. And with every restatement of it -- whether by a security check, a change of locks, the testing of alarms, a systems audit or a notice on the bulletin board -- you can be assured that you are influencing that moment of decision when an employee is faced with the choice to steal or not to steal.

Secure the Premises

Owner-managers who are haphazard about physical security -- i.e., issuing keys, locking doors and changing locks -- are, in effect, inviting the dishonest employee into the plant or office after work. Intelligent key control and installation of time locks and alarms are ways of serving notice to crooked workers to play it straight.

The more doors a plant has, the more avenues of theft it offers. For example, one stock clerk parked his car at the receiving dock. He kept the trunk closed but unlocked. At 12:30, when the shipping-receiving manager was at lunch, the stock clerk threw full cartons of shoes into the trunk and then slammed it locked. Elapsed time: 18 seconds.

A plant designed for maximum security will have a minimum number of active doors and a supervisor or guard, as warranted, stationed near each door. Moreover, a supervisor should be present when materials or finished goods are being received or shipped and when trash is being removed. As long as a door stays open, a responsible employee, supervisor or guard should be there.

Central station alarm systems should be used to protect a plant after hours. Their purpose is to record door openings and closing that can be investigated later if necessary. Time locks are also designed to record all openings.

Breakouts

A record of door openings can be important because the dishonest employee is often a specialist at breaking out, i.e., hiding inside and then leaving the plant after closing hours. If your plant is not protected against break out, you can be hurt badly, because this method of operation allows a thief to work essentially at his or her own speed.

After-hours thieves bypass the alarm system that works beautifully against break-ins. They can often leave by doors equipped with snap-type locks, i.e., doors that do not require keys from the inside. Quickly and easily, they can pass goods outside and close the doors behind them, leaving no evidence.

A motion detector, electric eye or central station alarm will deter such thieves. You can also discourage breakouts with locks that need keys on both sides, provided that local or state fire regulations do not prohibit such locks. When goods, materials or money are missing and there is

no evidence of forced entry, look for the inside thief.

Implement Audit Control Methods

Loss-prevention controls and procedures by themselves are not enough to protect your assets. Controls and procedures must be audited from time to time or they will break down. No loss-prevention control is stronger that its audit.

An effective auditing method is to omit deliberate errors. What will your people do if, for example, you see that more finished goods than the shipping order calls for reach the platform? Will the shipping clerk return the excess to stock? Will he or she try to divert it for personal use (perhaps in collusion with a truck driver)? Or will the clerk simply ship the order without ever knowing that the excess existed?

If the bookkeeper and the accounts receivable clerk are not dependable, alert and honest, disaster can result. Check them by withholding an invoice from each of them and observing their reaction. Will they miss the invoice? Will they realize that a missing invoice means lost revenue and call it to your attention?

Unannounced inspections are another excellent method of checking your preventive procedures. Such inspections are most effective during overtime periods or when the second or third shift is working. For example, one owner-manager popped up on the shipping platform after the second shift left. He noticed a loaded truck parked at the platform and ordered it unloaded. The cartons in the rear were legitimate deliveries, but he found the front half of the truck crammed with stolen goods. The checker, who was hired to see that such stealing did not happen, had gone to sleep and let the accommodating driver load his own truck.

Keep Crooks off Balance

The employees who are the most successful at their second trade are the ones who test the system and are convinced that they can beat it. With every score, their confidence increases and along with it their danger to the company. The best way to stop such crooks is to keep them off balance -- keep them from developing the feeling that they can beat your system.

Here's an example of how one owner-manager accomplished this. When inventory shrinkage became a major problem, he made a loss-prevention survey. To help keep employees honest, he reduced the number of exits employees could use by half. He performed unscheduled locker inspections at the most unlikely times.

Employees were no longer allowed to take lunch boxes or bags of any kind to their work stations. Package inspection procedures were tightened. To date, this owner-manager has caught no thieves. But by simply tightening controls and adding a number of surprise elements to his loss-prevention maintenance system, he reduced his inventory loss drastically.

Don't Play Detective

Owner-managers who suspect theft should not attempt to solve the crimes themselves. Even the best business owner may botch a criminal investigation because he or she is an amateur. When you suspect a theft, bring the police or a reliable firm of professional security consultants into the picture without delay. Where dishonest employees are bonded by insurance companies, ironclad evidence of theft must be uncovered before you can file a claim to recover your losses. Professional undercover investigation is among the most effective ways to secure such evidence.

Rules That Can Help Eliminate Employee Dishonesty

- ! Prosecute employees who are caught stealing. Settling for restitution and an apology is inviting theft to continue.
- ! Rotate security guards. Rotation discourages fraternizing with other employees who may turn out to be dishonest. Rotation also prevents monotony from reducing the alertness of guards.
- ! Price items by machine or rubber stamp, not by handwriting.
- ! Permit only authorized employees to set prices and mark merchandise.
- ! In cases of returns and refunds, insist on a merchandise inspection and approval by someone other than the person who made the sale.
- ! Pay special attention to cashiers when they are surrounded by clusters of people.
- ! Be alert to the use of over-ring slips to cover up shortages.
- ! Make a dependable second check of incoming materials to rule out the possibility of collusive theft between drivers and receiving personnel. Do not allow a truck to approach the loading platform until it is ready to load or unload.
- ! Do not allow drivers behind the receiving fence. Discourage drivers from taking goods or materials from the platform by the following devices: install heavy gauge wire fencing between bays, with the mesh too fine to provide a toehold; mount closed-circuit television cameras overhead that will sweep the entire platform; and locate the receiving supervisor's desk or office to give him or her an unobstructed view of the entire platform.
- ! At the loading platform, do not permit drivers to load their own trucks, especially by taking goods from stock.
- ! Make sure that every lunchbox, toolbox, bag or package is inspected by a supervisor or guard as employees leave the plant.
- ! Insist that all padlocks be snapped shut on hasps when not in use to prevent

switching of locks.

- Control keys to padlocks. Never leave the key hanging on a nail near the lock where a worker can borrow it and have a duplicate made while he or she is away from work.

- Do not allow trash to accumulate in, or be picked up from, an area near storage sites of valuable materials or finished goods.

- Supervise trash pickups and inspect disposal locations and rubbish trucks at irregular intervals for the presence of merchandise when you have the slightest reason to suspect collusion between employees and trash collectors.

- Control receiving reports and shipping orders (preferably by sequential numbering) to prevent duplicate or fraudulent payment of invoices or padding or destruction of shipping orders.

- Make sure that receiving reports are prepared immediately upon receipt of shipment. Delay in making out such reports can be an invitation to theft or, at best, result in record keeping errors.

EMBEZZLEMENT

You may not have had any experience with embezzlers but it is not uncommon. Every day there are newspaper stories about how an employee has managed to divert company funds to his or her own pocket. It happens often enough to make it worth your while to give the subject some thought and to examine your record keeping and auditing procedures to make sure there are no tempting loopholes.

Embezzlement is the fraudulent appropriation of property by a person to whom it has been entrusted. The key word is entrusted. That's what makes this crime different from ordinary theft or larceny. The embezzler is someone in your company whom you trust. In many cases the embezzler has been given more authority than the position calls for. Methods of embezzling are limited only by imagination.

You need a system of internal control to safeguard money and other property subject to embezzlement. Nobody wants to run a business like an armed camp, but if you have a built-in control system, administer it tightly and audit it frequently, you may prevent embezzlement attempts. At the least, you will have the means to collect evidence that may expose a crime.

Embezzlers usually think that they are smarter than the owner-manager and cunning enough to beat the system. Before you set about to outwit them, it is a good idea to be familiar with some of their methods of operation.

Some Common Schemes

Simple Embezzlement

In the simplest situation, cash is received and the employee merely pockets it without making a record of the transaction. A theft of this type is difficult to prevent or detect if the transaction is a cash sale and no subsequent entry is necessary in receipt or accounts receivable records. To reduce temptation, prenumbered sales invoices or cash register receipts should be used for all sales regardless of the amount. Spot checks and other monitoring procedures can also help assure you that cash sales are actually being recorded.

Lapping

A somewhat more complicated type of embezzlement is called lapping. This involves the temporary withholding of receipts, such as for payments on accounts. Lapping is a continuing scheme that usually starts with a small amount but can run into thousands of dollars before it is detected. For example, take an employee who opens mail or otherwise receives cash and checks as payment on open accounts. The employee holds out a $100 cash payment made by a customer A on March 1. To avoid arousing suspicion on A's part, $100 is taken from a $200 payment made by customer B on March 5. This is sent on, together with the necessary documentation, for processing and crediting to the account of A. The embezzler pockets the remaining $100, which increases the overall shortage to $200.

As this borrowing procedure continues, the employee makes away with increasingly larger amounts of money, involving more and more accounts. A fraud of this nature can run on for years. Of course, it requires detailed record keeping by the embezzler in order to keep track of shortages and transfer money from one account to another to avoid suspicion. Any indication that an employee is keeping personal records of business transactions outside your regular accounting books should be looked into.

Sometimes an embezzler who is carrying on a lapping scheme also has access to accounts receivable records and statements, and is thus in a position to alter the statements mailed out to customers. The fraud may continue undetected over a long period of time, until something unusual happens. A customer complaint may spotlight the situation or the matter may be surfaced through audit procedures such as confirmation of accounts receivable. One embezzler who also handled customer complaints was able to avoid detection for many years. The amount of the shortage reached such proportions and covered so many accounts that he dared not take a vacation. He even ate lunch at his desk lest some other employee receive an inquiry from a customer concerning a discrepancy in a statement. The owner-manager for whom he worked admired his diligence and loyalty and fellow workers marveled that his apparent frugality enabled him to enjoy a rather high standard of living. But the inevitable finally happened. The employee was hospitalized, and in his absence his fraudulent scheme came to light. One reason many firms require regular vacations is to keep some indispensable employee from dispensing with company funds illegally.

Check Kiting

Sometimes company bank accounts are used for check kiting. In fact, losses from some large check kiting schemes have been great enough to cause a company to go broke.

In the usual scheme, the check kiter must be in the position to write checks on and make deposits in two or more bank accounts. One account could be the embezzler's personal account and the other a business checking account. If the embezzler has an accomplice in another business, two business accounts may be used. If your company has more than one checking account at different backs, these accounts may be used to carry out the fraud.

The check kiter takes advantage of the time period between deposit of a check and collection of funds, also called the float period. Assuming that it takes three business days for checks to clear, a simple kite between two banks could be accomplished as follows:

On December 1, a check in the amount of $5,000 drawn on bank A is deposited in bank B. On December 2, the check kiter cashes a $5,000 check payable to cash, drawn on bank B. Since the original kited check will be presented for payment to bank A on December 4, the check kiter will deposit on or before that date a $6,000 check drawn on bank B in bank A, not only to ensure payment of the original kited check but also to increase the amount of the kite. As the process is repeated the kited checks become larger and more cash is withdrawn; and the scheme can continue until the shortage is covered -- or until the kite breaks when one of the banks refuses to honor a kited check because the funds on deposit are uncollected.

A dishonest employee may conceal a cash shortage at the end of a period by depositing a kited check into your company account. This brings the bank balance into agreement with the books. CPAs will request cut-off bank statements to detect frauds of this type.

Payroll Fraud

Payroll frauds are another source of loss to management. Occasionally, an enterprising embezzler has added the names of relatives or fictitious individuals to the company payroll and has thus enjoyed several salary checks each week instead of one.

Fraudulent Sales

Sometimes, when a company becomes so large that the owner-manager can no longer exercise personal surveillance of accounting activities, opportunities arise for a dishonest employee to set up a dummy supplier and falsify documentation of fictitious purchase transactions.

Other Means

Dishonest employees can figure out any number of ways to defraud their employers.

- Purchasing agents can accept kickbacks from suppliers from purchasing goods at inflated prices.

- Salespeople and others can pad their expense accounts.
- Personal items can be bought and charged to the company.
- Cashiers in retail firms can undercharge relatives or friends for merchandise.
- False vouchers can be prepared to conceal thefts from petty cash funds.
- Overtime can be falsely recorded.
- Employees can make personal use of company postage stamps, supplies and equipment, as well as charging personal long-distance phone calls to the business.

Make Your System Fraud Proof

The first thing an owner-manager should do is set a good example. Your employees watch what you do and tend to imitate your habits -- good or bad. An employer who dips into petty cash, fudges on an expense account, uses company funds for personal items or sets other examples of loose business behavior, will find employees rationalizing dishonest actions with the attitude If it's okay for the boss, it's okay for me.

An adequate accounting system with appropriate internal controls is your principal means for preventing and detecting fraud. Have a public accountant set it up; then be sure it is tested and evaluated at least annually by the auditor. Periodic examination will ensure that there are no loopholes through which an embezzler can manipulate your funds.

Design your auditing system to help document evidence in the event someone does try to embezzle. One problem in fidelity loss claims is proving the amount that was stolen. The owner-manager has to support a loss claim with evidence from the company's records.

You should insist that your accounting system provide you with at least monthly operating statements. These will inform you of the operations to date and the firm's financial condition. You can use these documents to compare the figures with prior periods. Any unusual or unexplained variations should be discussed with your accountant.

Another fundamental control is separation of the duties of employees. For example, persons concerned with receiving checks and cash should not also be responsible for making entries in the accounts receivable records. No one person should handle a transaction from beginning to end. If you do not exercise tight control over invoices, purchase orders, discounts and customer credits, you are asking for trouble.

Clues to Possible Embezzlement

Some kinds of business problems may be signs of embezzlement. Here are a few clues that indicate either an embezzler is at work in your company or certain aspects of the business need more of your attention.

- *Increase in overall sales returns* could be caused by defective merchandise -- or it might represent concealed accounts receivable payments.

- *Unusual bad debt write-offs* can be due to a number of business reasons -- or could be covering up a fraudulent scheme.

- *A decline or unusually small increase in cash or credit sales* might mean that business has not been good -- or it could mean that some sales are not being recorded.

- *Inventory shortage* can be caused by error or mismanagement -- or could indicate fictitious purchases, unrecorded sales or employee theft.

- *Profit declines and/or increases in expenses* can be entirely legitimate -- or could be a sign that cash is being siphoned of illegitimately.

- *Slow collections* can be caused by business conditions -- or can be a device to mask embezzlement.

Means of Preventing Embezzlement

There are many steps an owner-manager can take to cut down on the possibility of losses through embezzlement.

- *Check the background of prospective employees*. Sometimes you can satisfy yourself by making a few telephone calls or writing a few letters. In other cases, you may want to turn the matter over to a credit bureau or similar agency to run a background check. (Keep in mind that individuals' rights must be preserved in furnishing, receiving and using background information.)

- *Know your employees*. Know them to the extent that you may be able to detect signs of financial or other personal problems. Build up rapport so that they feel free to discuss such things with you in confidence.

- *Control your payroll*. See that no one is place on the payroll without authorization from you or a responsible official of the company. If you have a personnel department, require that it approve additions to the payroll as a double check. Have the preparation of the payroll and the actual paying of employees handled by different persons, especially when cash is involved.

- *Have the company mail addressed to a post office box rather than your place of business*. In smaller cities, the owner-manager may want to go to the post office to collect the mail. In any event, you or your designated key person should personally open the mail and record at that time cash and checks received. Don't delude yourself that checks or money orders payable to your company can't be

converted into cash by an enterprising embezzler. Also, arrange for bank statements and other correspondence from banks to be sent to the same post office box.

! *Supervise daily cash deposits*. Either personally prepare the daily cash deposits or compare the deposits made by employees with the record of cash and checks received. Make sure you get a copy of the deposit slip or other documentation from the bank. Make it a habit to go to the bank and make the daily deposit yourself as often as you can. If you delegate these jobs, make an occasional spot check to see that nothing is amiss.

! *Bank statement reconciliation*. Personally reconcile all bank statements with your company's books and records. The owner-manager who has not reconciled the statements for some time may want to get orientation from the firm's accountant.

! *Examine transaction documents*. Personally examine all canceled checks and endorsements to see if there is anything unusual. This also applies to payroll checks.

! *Bond your employees*. Make sure that an employee in a position to mishandle funds is adequately bonded. Let employees know that fidelity coverage is a matter of company policy rather than any feeling of mistrust on your part. If would-be embezzlers know that a bonding company also has an interest in what they do, they may think twice before helping themselves to your funds.

! *Spot check records*. Spot check your accounting records and assets to satisfy yourself that all is well and that your plan of internal control is being implemented.

! *Control outgoing funds*. Personally approve unusual discounts and bad debt write-offs. Approve or spot check credit memos and other documentation for sales returns and allowances. Don't delegate the signing of checks and approval of cash disbursements unless absolutely necessary and never approve any payment without sufficient documentation or prior knowledge of the transaction. Don't sign blank checks. Don't leave a supply of signed blank checks when you go on vacation.

! *Control invoices*. Examine all invoices and supporting data before signing checks. Make sure that all merchandise was actually received and the price was reasonable. In many false purchase schemes, the embezzler neglects to make up receiving forms or other records purporting to show receipt of merchandise. Personally cancel all invoices at the time you sign the check to prevent double payment, through error or otherwise.

! *Examine checking account items*. Inspect all prenumbered checkbooks and other prenumbered forms from time to time to insure that checks or forms from the

backs of the books have not been removed and possibly used in a fraudulent scheme.

Computer-related Crime

Small businesses are learning the many advantages of computers in every aspect of their operations. It is not unusual for the entire business to depend on computerized data. Personnel records, tax records, inventories, receivables, payables, shipments, bank accounts and all other vital records are contained on small diskettes that easily fit in a pocket. In such a concentrated form, business records are extremely vulnerable to removal or destruction. If something should happen to those diskettes, it could have the same effect as the sudden disappearance of significant business records and files.

Potential Impact of Computer Crime

Computers may facilitate crime. People with access to computerized data have the very pulse of your business at their fingertips. Dishonest employees can, and have, diverted funds and goods for their personal grain. If adequate security procedures are not followed, your entire business maybe at risk, and fraud can be difficult to detect or trace until it is too late. A disgruntled employee or an intruder can destroy unprotected computer files or diskettes in seconds, seriously impairing your business.

You can use computers to transfer funds, control inventory or process customers' orders. These same technologies, however, increase opportunity for unauthorized access to business data. *Hackers*, people who use their own computers and telephones to gain access to computerized data, may become an extremely serious problem. If you do not take elementary security measures, you can become their target; if they gain access to your business records, they can steal valuable proprietary information, divert your money or goods or destroy your records -- with a surprisingly small chance of being caught.

Consider the impact on your business if you were the victim of such intentional acts:

- Alteration of financial records for monetary gain.
- Malicious destruction of business records to get even.
- Insertion of unauthorized codes into commonly used software to perform unintended and unauthorized functions.
- Unauthorized use of a computer system for personal gain.
- Theft of computer equipment, data or programs.

These events generally result in a loss of confidentiality, integrity or availability of data or computer applications. While direct effects can immediately disrupt the business, longer term indirect effects can have a disastrous impact. For instance,

- Disclosure of proprietary business plans, product designs, costs, market data or customer lists can lead to a loss of competitive advantage in the marketplace, financial loss and lost opportunities.

- Fraudulent modification of inventory or other financial records, malicious modification of critical business data, or intentional errors introduced into source data, which then propagate throughout all business records, can result in significant losses.

- Unavailability of business information on computer resources can cause major business disruptions. Most businesses understand the impact on day-to-day operations of a key individual not reporting to work for several days, or of the unavailability of important support equipment (e.g., the lifts in an automobile service station). However, many small businesses underestimate (or fail to recognize) their dependence on computerized information and the continuity of computer processing capability. The impact of these situations can be devastating.

Securing Computers

The same characteristics of a computer system that expose your organization to large risks can offer significant business protection. Using computers will increase control much more than risks. The risks inherent in the use of a computer can be reduced to a minimum with procedures that are usually quite simple.

Protective steps to minimize computer risk include

- Establishing information security as a management priority.

- Identifying information resources and determining your vulnerability to and the potential impact of losses.

- Selecting and implementing administrative, equipment, information and data, software development and acquisition, and backup and contingency planning control measures to reduce potential losses.

- Monitoring results.

For more detailed information on preventing computer crime, please refer to the Small Business Administration (SBA) publication LF-OOl, *A Small Business Guide to Computer Security*.

Unauthorized Use of Facsimile Machines

Facsimile (fax) machines allow a business to transfer and receive documents over telephone lines. While unauthorized use of fax machines cannot cause as much damage as computers can, such use can result in excessive telephone bills. To avoid these problems,

- ! Establish strict procedures for fax machine use.
- ! Limit access to fax machines by installing them near authorized employees.
- ! Avoid using fax machines for confidential documents.
- ! Instruct employees to handle faxed documents as private communications.

If You Suspect a Crime

In the case of suspected embezzlement, first be sure that you do not jump to any unwarranted conclusions. What may appear to be embezzlement may, on further investigation, turn out to have a perfectly valid explanation. A false accusation could result in serious civil liability. There have been cases in which employees have been charged with embezzlement, dismissed from their positions and later found to be entirely innocent.

If you have good reason to suspect embezzling, contact your attorney immediately for guidance so that you will not subject yourself or your company to charges of false arrest. Discuss the necessity of notifying the bonding company and appropriate law enforcement authorities.

Don't subject yourself to criminal charges by helping conceal the commission of a crime. Embezzlers should be prosecuted when the facts so warrant and when there is sufficient evidence. These and other legal questions are best left to your attorney.

Summary

There are three principal ways to minimize the possibility of embezzlement losses. None is completely effective without the others. (1) internal controls -- perhaps the most effective safeguards against fraud; (2) independent audits -- discourage fraud and may uncover it; and (3) fidelity coverage -- can help you recover what may be lost in spite of your best efforts to prevent embezzlements.

SHOPLIFTING

Petty thievery may not seem like a major crime to the casual crook who pockets a ballpoint pen here, a pocket calculator there. But to the small business fighting for survival, it's murder. Just to cover a yearly loss of $1,000 in thefts, a retailer would have to sell each day over 900 candy bars, 130 packs of cigarettes or 380 cans of soup. Faced with such unreasonable selling volumes, most small business people are forced instead to raise their prices and lower their ability to compete.

Who Is a Shoplifter

What does a shoplifter look like? Like you. Or like me. Shoplifters can be male or female, any

race or color, as young as five or well into their 80s. Anyone who deliberately takes merchandise from a store without paying for it is a shoplifter, whether the theft is large or small, premeditated or impulsive.

Fortunately for business people, most shoplifters are amateurs. To the wary eye, they are not difficult to spot and, with the right kind of handling, may never try petty thievery again. Here are the various types of shoplifters:

Juvenile Offenders

Young people account for about 50 percent of all shoplifting. They may steal on a dare or simply for kicks. Frequently they expect store owners and courts to go easy on them because of their youth. They may enter stores in gangs in an attempt to intimidate management. Shoplifting is usually the first type of theft attempted by juveniles, and it may lead to more serious crimes. Youth is no excuse for crime, and the adult who lets it slip by is not doing the youngsters any favor. Juvenile theft should be pursued and prosecuted through the proper legal channels.

Impulse Shoplifters

Many respectable people fall into this category. They have not premeditated their thefts, but a sudden chance (such as an unattended dressing room or a blind aisle in a supermarket) presents itself and the shopper succumbs to temptation. The retailer can combat impulse shoplifting most effectively by simple prevention: building deterrents into the store layout and training employees to be aware of the problem and effective in dealing with it.

Alcoholics, Vagrants and Drug Addicts

An urgent physical need can drive people to theft, as well as to other crimes. These criminals are often clumsy or erratic in their behavior and may be easier than other types of shoplifters to detect. The store owner should remember, however, that people under the influence of drugs or with an obsessive physical need may be violent and/or armed. It is best to leave the handling of such people to the police.

Kleptomaniacs

A driving psychological need can lead a person to shoplifting. Kleptomaniacs are motivated by a compulsion to steal. They usually have little or no actual use for the items they steal and in many cases could well afford to pay for them. It is not up to the businessperson to make a psychological diagnosis. Shoplifting is shoplifting. It is no less costly simply because it is involuntary.

Professionals

Since the professional shoplifter is in the business of theft, he or she is usually highly skilled and hard to spot. Professionals generally steal items that will quickly be resold to an established fence. They tend to concentrate on high-demand, easily resold consumer goods such as

televisions, stereos and other small appliances. The professional, or booster, may case a store or department well in advance of the actual theft. While professionals may be hard to prosecute (they may belong to underworld organizations very effective in raising bail and providing defense in court), they can be deterred from theft by effective layout and alert personnel.

Methods of Shoplifters

Shoplifters may work alone or in groups. While it's impossible to give an infallible rule of thumb, experience has shown that juveniles and professionals tend to work in groups, while the impulse shoplifter is a loner.

The shoplifter may use confederates to be concealed. Gang members may distract sales help, start an argument with store personnel or among themselves, or even feign a fainting spell to draw attention, giving a cohort the opportunity to steal merchandise from another part of the store.

Shoplifters don't like crowds. They keep a sharp eye out for other customers or store personnel; quick, nervous glances may be a giveaway. They also tend to shop when staff coverage is lighter than usual, such as lunchtime, early morning or just before closing.

Shoplifters have an arsenal of professional tools. Articles as innocent as bulky packages, pocketbooks, baby carriages, knitting bags, shopping bags, umbrellas, newspapers and magazines can be used to carry stolen goods. Even an oversized arm sling can help the shoplifter conceal merchandise. Specially constructed devices, such as coats or capes with hidden pockets and zippered hiding places, are used by more experienced shoplifters. Some thieves use booster boxes (large boxes with a hinged end, top or bottom). Booster boxes can even be gift wrapped to frustrate detection.

Unsupervised dressing rooms offer excellent opportunities for theft. Shoplifters simply pile on layers of clothing, or they may exchange new items for the clothes they were wearing and return their own clothes to the rack.

Price tickets often can be easily switched, particularly in grocery stores or drugstores where prices are written on gummed labels and -- often carelessly -- stuck to the item.

Deterring Shoplifters

Your time and money are better spent preventing crime than prosecuting it. There are three major areas in which deterrence efforts pay off royally for the store owner.

1. Educate your employees. Train your sales staff to be alert to early warning signals. They should watch for customers carrying the concealment devices mentioned above, or walking with short or unnatural steps due to items being concealed between their legs.

2. Plan store layout with deterrence in mind. Maintain adequate lighting in all areas of the store. Keep protruding wings and displays low, not more than two or three feet high. Set

display cases in broken sequences.

Keep small items of high value (film, cigarettes, small appliances) behind a counter or in a locked case with a salesclerk on duty. Keep displays neat; it's easier to spot an item missing from an orderly array.

Attach noise alarms to unlocked exits. Close and block off unused checkout aisles. If you are involved in store design, plan to have entrances and exits in a common vestibule.

3. Use protective personnel and equipment. Protective devices may not be cheap, but shoplifting is costlier. You can get an idea of how much you can expect to lose to thieves by multiplying the number of shoplifters apprehended last year in your store by the average value of the stolen merchandise, then multiplying that figure by 50 weeks. The total is usually far greater than the cost of the deterrence systems.

Some of the most widely used devices are two-way mirrors, peepholes, closed-circuit television, convex wall mirrors and detectives posing as customers. To be valuable, surveillance devices must be properly placed and monitored. Uniformed guards can also be powerful visual deterrents to the shoplifter.

There are several ways to identify merchandise as having been legitimately paid for. One is to instruct cashiers to staple receipts to the outside of the packages. Electronic tags that trigger alarms at a store's exit may be attached to soft articles, such as clothing, to be removed only by a cashier with special shears.

If you use electronic sensing devices, be sure cashiers are diligent in removing the electronic tags. If they forget and the customer is falsely accused of shoplifting, you could be liable to charges of false arrest.

Two-way radios make it easy to stay close to suspected shoplifters and to alert security personnel.

Ticket-switching can be discouraged through the use of tamper-proof gummed labels, hard-to-break plastic sting, multiple price tickets concealed on items or special staple or punch patterns on price tags. Prices marked by rubber stamps or pricing machines are better than handwritten price tags.

Apprehension, Arrest and Prosecution of Shoplifters

While good deterrent systems will greatly reduce shoplifting, there are always people who are too dumb or too smart to be deterred. They'd try to steal the teeth out of a tiger's mouth if they thought the tiger wasn't looking. These people could force you to the last line of defense for your store. Remember, to give shoplifting charges a chance of sticking, you must be able to

- See the person take or conceal merchandise.

- Identify the merchandise as yours.
- Testify that it was taken with the intent to steal.
- Prove that the merchandise was not paid for.

If you are not able to meet all four criteria, you leave yourself open to countercharges of false arrest. False arrest need not mean police arrest; simply preventing a person from conducting normal activities can be deemed false arrest. Furthermore, any physical contact, even a light touch on the arm, may be considered unnecessary and used against you in court.

Check the laws in your state. Many states have passed shoplifting laws that deal with apprehension. Your lawyer or local police can advise you. Also, always consider your safety and that of your employees first and foremost.

In general, store personnel should never accuse customers of stealing, nor should they try to apprehend suspected shoplifters. If they observe suspicious behavior or an apparent theft in progress, they should alert the store owner, manager, store detective or police.

It is wisest to apprehend shoplifters outside the store. You have a better case if you show that the shoplifter left the store with stolen merchandise. Outside apprehension also eliminates unpleasant scenes that might disrupt normal store operation. You may prefer to apprehend shoplifters inside the store, if the merchandise involved is of considerable value or if you feel that the thief may be able to elude you outside the store premises. In either case, avoid verbal accusation of the suspect. One recommended procedure is to identify yourself and then say, I believe you have some merchandise that you forgot to pay for. Would you mind coming with me to straighten things out?

When cornered, the first thing most shoplifters -- impulse thieves or professionals -- will say is, I've never done this before. In general, this is all the more reason, if your evidence is sufficient, to call the police and proceed with prosecution. Failure to prosecute first-time offenders encourages them to try again. Word also gets around that your store is an easy hit.

Some organizations have control files on shoplifters who have been caught. Your retail merchants' association can inform you about the services available in your area. You can check these files to see whether the person you catch has a prior record. A shoplifter who claims to be a first offender is likely to remain a first offender unless you get positive identification and file his or her name with the police and local retail merchants' association.

Naturally, each situation must be handled differently and your good judgement is required. You may wish to release elderly or senile shoplifters and not press charges where there's some indication that the person could honestly have forgotten to pay for the merchandise. In most cases, however, prosecution is in order. It is essential if the shoplifter is violent; if he or she lacks proper identification and you suspect a prior record; if he or she appears to under the influence of alcohol or other drugs; if the theft involves merchandise of great value; or if the shoplifter appears to be a professional.

Juvenile shoplifters require special handling. A strict, no-nonsense demeanor often makes a lasting impression on the young offender and may deter future theft. Many stores choose to contact the parents of young shoplifters rather than the police; but, remember, juveniles account for half of all shoplifting that goes on in this country. The parents of troubled youngsters may be ineffective in handling the situation. Whom are you helping if you let the young shoplifter steal again?

BAD CHECKS

A neatly dressed stranger pays for her groceries with a payroll check issued by a company in a nearby city. In the next few hours, she does the same thing in several other food stores. In another community, a middle-aged man pays for a pair of shoes with a government check. He moves to other stores and cashes several more government checks. In a third city, a well-dressed woman pays for an expensive dress with a blank check. I need a little pocket cash, she says. May I make the check for $20 more? The salesclerk agrees, never suspecting that the customer does not have an account in any bank.

Tomorrow, these three con artists will work in other communities. The specialist in payroll checks will fill out blank ones she has stolen. The passer of government checks is also a thief. He steals social security checks, tax refund checks and so on from individual mail boxes. Blank Check Bessie will hit her victim after the banks have closed. These three, and others who pass worthless checks, are clever. They live by their wits and are often glib talkers. But they are not so clever that you can't outwit them.

Types of Checks

Winning the battle of wits against those who pass bad checks is largely a matter of knowledge and vigilance. You have to know what you're up against, pass the information on to your employees and be constantly on guard when accepting checks.

You are apt to get seven different kinds of checks: personal, two-party, payroll, government, blank, counter and traveler's. Some customers may offer money orders.

A *personal check* is written and signed by the individual offering it. The individual makes it out to you or your firm.

A *two-party check* is issued by one person, the maker, to a second person, who endorses it so that it may be cashed by a third person. This type of check lends itself to fraud because, for one thing, the make can stop payment at the bank.

A *payroll check* is issued to an employee for wages earned. Usually the name of the employer is printed on it, it has a number and is signed. In most instances Payroll is also printed on the check. The employee's name is printed by a check writing machine or typed. You should not

cash a payroll check that is handprinted, rubber stamped or typewritten, even if it appears to be issued by a local business and drawn on a local bank, unless you are in a small community where you know the company officials and the employee personally.

A *government check* can be issued by the federal government, a state, a county or a local government. Such checks cover salaries, tax refunds, pensions, welfare allotments and veterans benefits, to mention a few examples. You should be particularly cautious with government checks. Often they are stolen and the endorsement has been forged. In some areas, such thievery is so great that some banks refuse to cash social security, welfare, relief or Internal Revenue Service checks unless the customer has an account with the bank. You should follow this procedure also. In short, know your endorser.

A *blank check*, sometimes known as a universal check, is no longer acceptable to most banks due to Federal Reserve Board regulations that prohibit standard processing without the encoded characters. This universal check may be used, but it requires a special collection process by the bank and incurs a special cost.

A *counter check* is still used by a few banks and is issued to depositors when they are withdrawing funds from their accounts. It is not good anywhere else. Sometimes a store has its own counter checks for the convenience of its customers. A counter check is not negotiable and is so marked.

A *traveler's check* is a check sold with a preprinted amount (usually in round figures) to travelers who do not want to carry large amounts of cash. The traveler signs the check at the time of purchase and counter-signs it in the presence of the person who cashes it.

In addition, a *money order* can be passed as a check. However, a money order is usually sent in the mail. Most stores should not accept money orders in face-to-face transactions. Some small stores sell money orders. If yours does, never accept a personal check in payment for money orders. If the purchaser has a valid checking account, why does he or she need a money order?

Key Items on Checks

A check carries several key items, such as name and location of the issuing bank, date, amount (in figures and spelled out) and signature. Close examination of such key items can sometimes tip you off to a worthless check. Before accepting a check, look for

- *Issuing bank* -- Use extra care in examining a check that is drawn on a nonlocal bank and require positive identification. List the customer's local and out-of-town address and phone number on the back of the check.

- *Date* -- Examine the date for accuracy of day, month and year. Do not accept the check if it's not dated, if it's postdated or if it's more than 30 days old.

- *Location* -- Look first to be sure that the check shows the name, branch, town and state where the bank is located.

- *Amount* -- Be sure that the numerical amount agrees with the written amount.

- *Legibility* -- Do not accept a check that is not legibly written. It should be written and signed in ink and must not have any erasures or written-over amounts.

- *Payee* -- When you take a personal check, have the customer make it payable to your firm. Special care should be used in taking a two-party check.

- *Amount of purchase* -- Personal checks should be for the exact amount of the purchase. The customer should receive no change.

- *Checks over your limit* -- Set a limit on the amount -- depending on the amount of your average sale -- you will accept on a check. When a customer wants to go beyond that limit, your salesclerk should refer the customer to you.

- *Low sequence numbers* -- Be more cautious with low sequence numbers. Experience indicates that more of these checks are returned. Most banks that issue personalized checks begin the numbering system with 101 and number in sequence when a customer reorders new checks.

- *Amount of check* -- Most people who pass bad checks do so in the $25 to $35 range, on the assumption that the retailer will be more cautious when accepting a larger check.

- *Type of merchandise purchased* -- Be aware of the type of merchandise purchased. Selection of random sizes or items, or a customer's lack of concern about prices may suggest that caution be used in accepting payment by check.

Procedures for Accepting Checks

Require Identification

Once your are satisfied that the check is okay, the question of whether the person holding the check is the right person remains. Requiring identification helps you to answer the question. But keep in mind that no identification is foolproof; it can be forged. Some stores require at least two pieces of identification. It is important to get enough identification so the person presenting the check can be identified and located if and when the check turns out to be worthless.

The following types of identification are useful in determining whether or not to accept a check:

- *Current automobile operator's license* -- If licenses in your state do not carry a photograph, you may want to ask for a second identification.

- *Automobile registration card* -- Be sure the name of the state on the registration agrees with the location of the bank on the check. If it doesn't, the customer should be able to explain why. Also, make sure that the signatures on the registration and check agree.

- *Shopping plates* -- If they bear a signature or laminated photograph, shopping plates or other credit cards can be used as identification. Retail merchants' associations in some communities issue lists of stolen shopping plates to which you should always refer when identifying a person presenting a check.

- *Government passes* -- These can be used for identification in cashing checks. Picture passes should carry the name of the employing department and a serial number. Building passes should also carry a signature.

- *Identification cards* -- Cards such as those issued by the armed services, police departments and companies should carry a photo, a description and a signature. Police cards should also carry a badge number.

Several types of cards and documents are not good identification. Some of them (for example, club cards) are easily forged, and others (for example, a customer's duplicate salescheck) were never intended for identification. Unless they are presented with a current automobile operator's license, do not accept the following:

Social security cards	Initialed jewelry
Letters	Work permits
Business cards	Unsigned credit cards
Birth certificates	Insurance cards
Club or organization cards	Voter registration cards
Library cards	Learner's permits
Bank books	Customer's duplicate cards

Some large stores photograph each person who cashes a check. This procedure is a deterrent because those who pass bad checks don't want to be photographed.

Some stores, when in doubt about a check, will verify an address and telephone number in the local telephone directory or with the directory assistance operator. Someone intending to pass a bad check will not necessarily be at the address shown on the check. If the address and telephone number cannot be verified, the check should be considered a potentially bad check.

Compare Signatures

Regardless of the type of identification you require, it is essential that you and your employees compare the signature on the check with the one on the identification. You should also compare the person standing before you with the photograph and or description on the identification.

Set a Check-Cashing Policy

You should set a policy for cashing checks, write it down and instruct your employees in its use. Your policy might require that you approve checks before they can be cashed. When all checks are handled alike, customers have no cause to feel that they are being treated unfairly.

Your procedure might include the use of a rubber stamp. Many stores stamp the lower reverse side of a check and write in the appropriate information. Below is a sample of such a stamp.

Your policy might also include verifying a check through the bank that issued the check. Some banks will do this only if you are a depositor in the bank. It might be helpful to establish business accounts in several banks, particularly where many of your customers have accounts.

You may want to verify a check through a check verification service. Should you contract with such a service or receive lists of persons who have passed bad checks, ask the service to show you proof from the Federal Trade Commission that their service is in compliance with the Fair Credit Reporting Act.

Employee apathy toward accepting checks is a major reason why stores are left with bad checks. The bigger the store, the more difficult it is to keep employees interested in catching bad checks. One effective way is to show employees your bad checks.

Refusing a Check

You are not obligated to take anyone's check. Even when a stranger presents satisfactory identification, you do not have to accept the check. In most cases, you accept a check when the customer has met your identification requirements. You want to make the sale. But never accept a check if the person presenting it appears to be intoxicated or acts suspicious. For example, the customer may try to rush you or your employees while you are checking identification. Never take a check that is dated in advance. And never discriminate when refusing a check. Don't tell a customer that you can't accept a check because he or she is a college student or lives in a bad neighborhood. If you do, you may be in violation of a state or federal discrimination law.

Recovering Funds from Bad Checks

Whether or not you recover any money lost on a bad check depends on the person who gave it to you. He or she may be one of your best customers who inadvertently gave you a check when the funds in his or her bank account were insufficient. On the other end of the scale, he or she may be a forger. Once you are stuck with a bad check, here are some of the situations you face.

Insufficient Funds

Most checks returned because of insufficient funds clear the second time you deposit them. Notify the customer that his or her account is overdrawn and that you are redepositing the check. But if the check is returned a second time, in some localities, it is the retailer's collection problem and you must try to get the customer to honor the check by paying immediately. Check the practices of your bank. Some stores prosecute if the customer does not redeem such a check

within a week of the second return. Stores with a reputation for being easy going about insufficient funds checks usually get plenty of them.

The procedure for prosecution depends on the state. In one jurisdiction, for example, a merchant must send the check writer a certified or registered notice of an intention to prosecute. The check writer then has five days from the date of receipt of that notice to comply before the merchant can prosecute. In another jurisdiction, the maker has five days after the date of notice to make the check good. In a third, a resident has ten days to make the check good.

No Account

Usually you've lost when the bank returns a check marked no account. Such a check is evidence of a swindle or a fraud unless there has been an extraordinary error. In rare instances, a customer may issue a check on the wrong bank or on a discontinued account. You should quickly determine the circumstances. If the person is known in the community, proceed with your collection efforts. If you find yourself stuck with the check, call your local police department.

Closed Account

A check marked closed account is a warning of extreme carelessness or fraud. Accounts are closed by both individuals and banks. The latter may close an account because of too many overdrafts. An individual may open a new account by removing funds from an old account. In such a case, the individual may forget that he or she has issued a check that is still outstanding against the old account. If you don't get your money back within a reasonable time, you should consider prosecuting the check writer.

Forgery

Forged checks are worthless -- a total loss to you. Watch for smudged checks, misspelled words or poor spacing of letters or numbers, indicating that changes may have been made. Payroll checks with the company's name and address typed in could be fraudulent; most payroll checks are printed.

When you suspect forgery, call the police. In this way, you can protect yourself and other against further forgery. Refer a U.S. government check to the field office of the U.S. Secret Service.

Check with your lawyer about court collection practices in your area. In the Washington, D.C. area, for example, merchants cannot collect through the courts on bad checks used to pay an open account; the reasoning being that the merchant still has the account and no injury was suffered through the issuance of the check. The account may be collectable through the usual civil procedures for collection purposes.

Any alteration, illegal signature(s) by the writer of the check, a forgery of the endorsement, an erasure or an obliteration on a genuine check is a crime.

A bad check issued to pay for merchandise is a misdemeanor. It is an exchange -- the check for goods. A misdemeanor may carry a lighter penalty than theft since a check may be collectable through civil procedures. Criminal action can be taken when you sign a formal charge with the police.

A forged check transported in interstate commerce is a federal offense.

Get Evidence

You cannot prosecute those who pass bad checks without good evidence. The person who cashed the check should be positively identified as having received money for it.

The Short-Change Artist

Short-change artists prey on all businesses, from service stations to the best hotels. As with all other con people, short-changers have a good working knowledge of human nature. They have confidence in their ability to outwit victims, and are smooth talkers using an unending line of chatter to distract victims. Several exchanges of money between the thief and victim must occur, during which the thief attempts to confuse the victim into surrendering more money than the thief is entitled to. Once the theft is accomplished, the thief departs before the victim realizes what has happened.

What to Watch For

Most popular is the double operation. The typical scheme runs as follows: the first operator makes a small purchase and tenders a large bill$10 or $20. The large bill may have a name, address, telephone number or other identifying information on it. This operator receives change from the cashier and departs. The second operator makes a similar small purchase, offers a small bill in payment and begins to engage the cashier in endless meaningless conversation. The cashier gives correct change. At this point, the second operator accuses the cashier of an error: the bill tendered was a large bill not a small bill. The cashier will, of course, claim otherwise. This operator then recites the information appearing on the bill presented by the first operator.

Minimizing the Risk

There are several variations of the short-change artist scam. To minimize your risk of becoming a victim

- Instruct cashiers to complete transactions carefully and close the cash register drawer immediately.
- Instruct cashiers to politely excuse themselves from unrelated conversation and devote full time attention to completion of the transaction.
- Should a dispute arise concerning an error in change, indicate that a manager

should be summoned immediately.

- Provide alternate procedures to opening a check-out cash register for customers needing change for large bills.

- Arrange check-out stations so no cashier is isolated.

BURGLARY AND ROBBERY

Small stores are prime targets for burglars and robbers. Seeking dark and easy-to-enter stores, burglars usually operate at night. Attracted by careless displays of cash, robbers often strike at opening or closing time or when customer traffic is light.

Because you may be the victim of a robbery or a burglary in your area, you should be aware of precautionary measures to lessen the impact of these two crimes.

Burglary

Burglary is any unlawful entry to commit a felony or a theft, even though no force is used to gain entrance.

Retailers whose stores have been broken into know that burglaries are costly. What these business owners may not be aware of is that the number of burglaries has doubled in the past several years and, therefore, they may be two-, three- or four-time losers if the trend is not reversed. Moreover, few burglars are caught; almost 80 percent of burglaries go unsolved. Arrest and prosecution are difficult because of a lack of witnesses or evidence to identify the criminal.

Prevention must start with the small merchant -- you. Use a combination of measures to protect your store from burglars, including

- Suitable locks.

- An appropriate alarm system.

- Adequate indoor and outside lighting.

- A secure store safe..

In addition, the owners of high-risk stores -- those in areas with a reputation for rampant crime -- should also consider using

- Heavy window screens.

- Burglar-resistant glass windows.

- Private police patrols.
- Watchdogs.

Locks

Be sure to use the right kind of lock on your doors. In addition to being an obstacle to unwanted entry, a strong lock requires a burglar to use force to get into the store. Under standard burglary insurance policies, evidence of a forced entry is necessary to collect on burglary insurance.

Most experts on locks agree that the pin-tumbler cylinder lock provides the best security. It may have from three to seven pins; locksmiths caution that a burglar can pick a lock with less than five pins. There are a few non-pin tumbler locks that give high security, but you should check with a locksmith before you use one.

Dead bolt locks (bolts that are moved by turning the knob or key without action of a spring) should be used. They cannot be opened by sliding a piece of flexible between the door edge and door jamb. When you use a double cylinder dead lock, the door cannot be opened without a key on either side. This fact means that on a glass door there is no handle for a burglar to reach by merely breaking the glass. Such a lock also provides protection against break-outs.

Safeguarding entranceways, especially the rear door, cannot be overemphasized. Bar the rear door, in addition to locking it, because burglars favor back doors.

Special situations may require consideration of state-of-the-art electronic lock systems. These locks are entered with coded cards that cannot be duplicated.

Installing Locks

The best lock is ineffective if it is not properly installed. For example, if a lock with a 5/8-inch long latch bolt is installed in a door that is separated from the door jamb by 1/2-inch, the effective length of the bolt is cut to only 1/8-inch. Have a locksmith check the locks on your exterior doors to be sure they give you the right protection.

Key Control

To keep keys from falling into the hands of burglars, issue as few keys as possible and keep a record of those you do issue. Exercise the same care with keys as you would with a thousand dollar bill:

- Avoid key duplication. Caution employees not to leave store keys with parking lot attendants, in a coat hanging in a restaurant or lying about the office or stockroom.
- Keep your records on key distribution up-to-date so you know what keys have been issued to whom.

- Whenever a key is lost or an employee leaves the firm without turning in his or her key, re-key your store.

- Have one key and lock for outside doors and a different key and lock for your office. It is not advisable to use master keys because they weaken your security. If you do, however, take special care to protect them.

- Have a code for each key so that it does not have to be visibly tagged and only an authorized person can know the specific lock that key fits. Don't use a key chain with a tag carrying the store's address.

- Take a periodic inventory of keys. Have employees show you each key so you will know it has not been lost, mislaid or lent.

Alarms

The silent central station burglary alarm system gives your store the best protection because it does not notify the burglar of detection as does the local alarm -- such as a siren or bell -- outside the store. A silent alarm alerts only the specialists who know how to handle burglaries.

In large cities, central alarm systems are available on a rental basis from private firms; in small cities, they are often tied directly into police headquarters. Part of the cost for installing a silent alarm system will sometimes be defrayed by a reduction in your burglary insurance premium.

Although a building-type local alarm is cheaper and easier to install, it too often only warns the thief and is not considered by specialists to be as effective as a central station alarm. Of course, if no central alarm service system is available, or such an alarm is not feasible, then by all means install a building alarm.

Whether your alarm is central or local, you have a wide choice of alarm sensing devices. Among them are radar motion detectors, invisible photo beams, detectors that work on ultrasonic sound and vibration detectors. Supplemental equipment, such as an automatic phone dialer, phones the police and the store owner and warns them that an alarm has been breached.

Each type of alarm has advantages in certain situations. Seek professional guidance to get the best alarm system for your needs.

Lighting

Outdoor lighting is another way to shield the store from burglary. Almost all store break-ins occur at night. Darkness conceals the burglar and gives him or her time to work. By floodlighting all around the outside of your store, you can defeat many burglars. Include alley entrances and side passageways between buildings where entry might be made.

Mercury and metallic vapor lamps are good for illuminating the exterior walls of a store. They

are designed to withstand vandalism and weather, such as wind velocities up to 100 miles per hour. Some have a heat-tempered lens that cannot be broken with less than a 22-caliber rifle.

Indoor lighting is also important. When a store is lighted inside, police officers can see people in the store or notice the disorder that burglars usually cause. When the store is dark, the burglar can see the police approaching, but the police can't see the burglar. Police get to know lighted stores and will check the premises when a light is off. It is also important to arrange window displays so police patrols can see into the store.

Your Safe

Be sure the safe in which you keep your money and other valuables is strong enough to deter burglars. A file cabinet with a combination lock is not a safe. Money should be protected in a burglar-resistant money chest.

Insurance companies recognize the E Safe as adequate for most merchant risks (except, in a few cities, where torch and explosive attacks on safes are common.) Insurance companies give a sizable reduction in premiums for use of the E Safe; over the years, these savings can pay the added cost of an E Safe.

Locating Your Safe

Putting a safe in the back of the store or where it is not visible from the street invites burglary. Police recommend that the safe be visible to the street outside and that the safe area be well lighted all night.

But visibility and lighting will be a wasted effort if your safe can be carted off by a burglar. Weight is no guarantee that the safe can't be stolen -- safes weighing 2,000 pounds have been taken out of stores. No matter what the safe weighs, bolt it to the building structure.

Leave the "cupboard bare."

Even when you use an E-rated burglar-resistant money chest, it is a good idea to keep on hand the barest minimum of cash. Bank excess cash each day.

Leave your cash register drawer empty and open at night. A burglar will into a closed one, and the damage to your register can be costly.

Use a silent central station alarm on your safe cabinet. When closing your safe at night, be sure to do the following:

- Check to see that everything has been put into the safe.
- Make a note of the serial numbers on large bills taken in after your daily deposit.
- Check to be sure that your safe is locked.

- Activate the burglar alarm.

Make it a practice never to leave the combination of your safe on the premises. Change the combination when an employee who knows it leaves your firm.

High-risk Locations

Some stores are in high-risk locations with a reputation for crime. Night after night, people break display windows and help themselves or force their way into stores.

Because many windows are smashed on impulse, you should minimize the chance of loss. If possible, remove attractive and expensive merchandise from the window at night. Many jewelry stores protect items left in the display window by secondary glass -- a piece of heavy glass hanging on chains from the window's ceiling. Being nonfixed, the secondary glass is difficult to break even if the burglar smashes the display window.

If your store is in a high-risk location, consider using heavy window screens, burglar-resistant glass, other points of entry, watchdogs or private police patrols.

Heavy Window Screens

Heavy metal window screens or grating are an inexpensive way to protect show windows. Store them during business hours, and, at closing time, put the screens up and lock them in place.

Burglar-Resistant Glass

When used in exterior doors, windows, display windows and interior showcases, this glass deters burglars. It has a high tensile strength that allows it to take considerable beating. This glass is a laminated sandwich with a sheet of invisible plastic compressed between two sheets of glass. It mounts like ordinary plate glass and is clear, tinted or opaque.

Of course, this type of glass can be broken with continual hammering -- as with a baseball bat or sledgehammer. But it will not shatter. The burglar who is patient enough to bang a hole in the glass will find it bordered by sharp jags.

Even in prestigious locations, burglar-resistant glass offers protection. It can be used in stores selling high value merchandise such as cameras, furs and jewelry.

Other Points of Entry

Look up to determine if you are vulnerable from above. Skylights, ventilators, roofs and roof hatches may not prove as inconvenient to a burglar as they seem to you. Indeed, they allow burglars added time to accomplish their goals without being detected.

The light, relatively thin nature of roofing materials is easy work for a determined burglar. Regular inspections and appropriate repairs and reinforcement are a must from a security standpoint. Critically evaluate the need for roof openings. Those with little value should be permanently sealed. Protect necessary roof openings with electronic hardware.

Watchdogs

In larger cities, agencies offer watchdog service for a nominal hourly fee. An owner-manager can use these dogs on a spot check basis one or two nights a week to deter burglars. Word soon gets around that a store is using watchdogs, and burglars cross the store off their list.

Private Police Patrols

A private police patrol can be used to supplement an undermanned or overworked police force. Such a patrol can discourage burglars by checking the store during the night. Private police may catch a burglar in the act or discover the break-in shortly after it occurs. In either case, their prompt notice to the police increases the likelihood of catching the culprit and recovering your merchandise and money.

A private patrol is also qualified to testify on the store conditions prior to a crime. This sort of testimony expedites the payment of insurance claims. In a disaster, such as a flood or riot, private police can initiate emergency measures.

A private patrol can also help you train your employees, and can point out unlocked doors, open windows and other signs of employee carelessness that can be corrected.

Visitor Access

The nature and size of your business will determine your need to control visitor access to all or portions of the premises. At potential risk are proprietary information, data, sensitive equipment and areas where cleanliness is crucial (e.g., laboratories).

Your policy should be written, easily understood by employees and visitors and uniformly enforced. Put up clear signs in your controlled areas and in your reception area.

Robbery

Robbery is stealing or taking anything of value by force, violence or threat.

Retailers who have been robbed several times are not surprised to learn that police call robbery the fastest growing crime in the nation. The greatest increase is in retail stores where holdups have increased 75 percent in the past several years. Only about one third of the robberies in the United States are solved by identification and arrest. Even when robbers are caught, almost none of the cash or property is recovered. Robbery is a violent crime. The robber always uses force or the threat of force, and the victims are often hurt. In 65 percent of store holdups, the robber uses

a weapon.

What can you do to reduce losses from robbery in your store? Your first line of defense is to train your people. How you handle your cash is also important. It is also vital that you use care in opening and closing your store and when answering after-hours emergency calls.

Train Employees to Reduce Risk

Let your employees know what may happen if a robbery occurs. Train them in how to respond. Emphasize the protection of lives as well as money. Warn each person that you want no heroes. The heroic action of an employee or customer may be a deadly mistake. The robber is as volatile as a bottle of nitroglycerin. Handle him or her with the same care you would any explosive.

Instruct your people to do the following if they face a robber:

- Reassure the robber that they will cooperate in every way.
- Stay as calm as possible.
- Make mental notes on the criminal's build, hair color, complexion, voice, clothing and any other identifying trait. A calm, accurate description of the robber can help bring him or her to justice. (Police advise that employees not discuss or compare descriptions with each other but wait until police arrive.)

Instruct your employees not to disclose the amount of loss. The police and news reporters should receive such information only from you. When talking to reporters, play down the theft. Don't picture your store as being an easy mark with a great deal of cash on hand.

Don't Build up Cash

Cash on hand is the lure that attracts a robber. The best deterrent is to keep as little cash in the store as possible. Make bank deposits daily. During selling hours, check the amount of cash in your registers. Remove all excess from each register several times a day.

Do not set up cashier operations so that they are visible to outsiders. The sight of money can trigger crime. Balance your register an hour or two before closing -- not at closing time. Make it a rule to keep your safe locked even during business hours.

When making bank deposits, use an armored car service, if practical. If not, take a different route to the bank each day and vary the time of the deposit. Obviously, the best time to make deposits is during daylight hours.

You should also vary the routes you travel between the store and your home. Keep your store keys on a separate key chain. At least then, in case of a robbery, you won't be stranded by the loss of your car and personal keys.

Opening and Closing Routine

Opening or closing the store is a two-person job. When opening your store, station one person -- an employee or your assistant -- outside where he or she can observe your actions. Enter the store, check the burglar alarm to be sure it is still properly set, then move around in the store and look for any signs of unwanted callers.

You and your assistant should agree on the length of time this pre-opening check is to take. If you do not reappear at the scheduled time, your assistant should phone the police. The outside person should always know where the nearest phone is located and should have a card with the police phone number typed on it and coins taped to the back so that he or she has the right change to make the call.

When phoning the police, the caller should calmly

- Give his or her name.
- Give the name and address of the store.
- Report that a holdup may be in progress at the store.

Under normal conditions, the owner-manager would return to the entrance after finishing the store inspection and give the outside person a predetermined all clear signal.

Your night closing should follow a similar routine. A few minutes before closing, make a routine check of stockrooms, furnace room, storeroom and other places where a thief might hide. A second employee should wait just outside the store until you have finished your inspection. If you drive to work, the employee should bring your car to a location near the exit door and should watch while you set the burglar alarm and lock the doors and windows.

Be Cautious of Night Calls

Whenever you receive an emergency call to return to the store at night, be careful.

- Never return to the store without first notifying someone that you are returning.
- If the call is triggered by a burglar alarm, phone the police department and ask that a police car meet you at the store.
- If it is a repair problem, phone the repair company and have the service truck sent out before you leave home.
- If you arrive at the store and do not see the police car or the repair truck, do not park near the store -- and do not enter the store.
- Make it a habit to verify all phone calls you receive after store hours, no matter

where they originate. A careless slip on your part may be all the criminal is waiting for.

SUMMARY

Security is an everyday, year-in-year-out responsibility.

Reading this or other security-related publications is only one step in protecting your business and your investment in it. You must carefully analyze all aspects of your business, identify potential vulnerabilities and take steps to minimize them. Use this publication as a tool.

Acquire the appropriate hardware.

- Locks.
- Lighting.
- Monitors.
- Alarm systems.
- Fences.

Act on the people-related aspects.

- Hiring policies.
- Money handling.
- Data processing.

Complete your program by

- Developing a written security policy, including steps to be taken in the event of an emergency or natural disaster and provisions for annual review and updating.
- Developing daily security routines (see Appendix A).
- Appointing a trusted employee to head your security effort and at least one backup to serve as a substitute.
- Drafting written rules on security for all employees.
- Conducting regular training sessions for your employees (see Appendix B).

APPENDIX A: CHECKLIST FOR DAILY SECURITY ROUTINE

Responsibility of _____

Backup_____

Alternate backup_____

Start of the work day

Opening inspection
- Burglar alarm off
- Check forced doors
- Check forced windows
- General order of entire premises
  - Stairwells
  - Elevators
  - Individual rooms
    - Customer service area
    - Utility/mechanical plant
    - Storerooms
    - Stockrooms
    - Rest rooms
    - Offices
    - Unsecured closets
- Safe
- Computers
- Daytime security devices on
  - Electronic tag monitors
  - Video cameras
- Report of findings/all clear
- Employee check in

During the Work Day

Money controls
- Cash registers
- Management office
- Cash deposit procedures
- Check reception
- Credit card reception

Customer monitoring
- Shoplifting alertness
- Scam alertness

- Loitering

Communications devices/intercom

Secure areas
- Loading dock/supply reception
  - Inventory control
  - Storerooms
  - Management office
  - Laboratories
  - Utility controls/mechanical plant

Handling of official inspectors

End of the work day

Employee checkout

Closing inspection
- Computers signed off
- Safe locked
- General order of entire premises
  - Stairwells
  - Elevators
  - Individual rooms
  - Customer service area
  - Utility/mechanical plant
  - Storerooms
  - Stockrooms
  - Rest rooms
  - Unlocked closets
- Windows checked
- Doors locked
- Daytime security devices off
- Automatic security lighting functioning
- Burglar alarm on
- Report of findings/all clear

After-hours operations

Access
Sign-in/sign-out
Computers

Operations during/after emergencies

Fire
Flood
Storm
Earthquake
Considerations for 24-hour operations
Security hotline
Cash handling
Access
Lighting

APPENDIX B: EMPLOYEE SECURITY TRAINING

Frequency -- Annual, following company's yearly review of security procedures for success/failure/needs improvement; periodic, following any major incident or emergency; small group, for new employees.

Suggested speakers (individually or in panels) -- Company president or top manager, company security chief (title or staff function), local police officer, legal counsel, security hardware consultant and insurance representative.

Suggested handouts -- Company security rules; excerpts from SBA publications on shoplifting, check handling, etc., or from other publications that you have permission to copy.

Sample Agenda for Security Training

Opening remarks on importance of employee role in security;
- encouragement of honesty and zero shortage attitude;
- encouragement of questions during session.

Company security rules (with handout)

Company security tools or hardware

Handling of money
- Short-change artists
- Payment by check
- Payment by credit card
- Payment with fake money

Shoplifting/employee theft
- What to watch for
- What to do

Robbery
- What to do

Scams

What to watch for (i.e., customers deliberately damaging merchandise then asking for discounts on the goods; fake inspectors, etc.)

What to do

Computers

Crimes of other employees

What to watch for (i.e., falsifying records; sabotaging machinery, etc.)

What to do when you see it

Alertness for conditions that jeopardize security

What to look for

What to do

Closing remarks encouraging honesty and alertness

APPENDIX C: INFORMATION RESOURCES

U.S. Small Business Administration (SBA)

The SBA offers an extensive selection of information on most business management topics, from how to start a business to exporting your products.

SBA has offices throughout the country. Consult the U.S. Government section in your telephone directory for the office nearest you. SBA offers a number of programs and services, including training and educational programs, counseling services, financial programs and contract assistance. Ask about

- *SCORE: Counselors to America's Small Business*, a national organization sponsored by SBA of over 11,000 volunteer business executives who provide free counseling, workshops and seminars to prospective and existing small business people. Free online counseling and training at www.score.org.

- *Small Business Development Centers (SBDCs)*, sponsored by the SBA in partnership with state governments, the educational community and the private sector. They provide assistance, counseling and training to prospective and existing business people.

- *Women's Business Centers (WBCs)*, sponsored by the SBA in partnership with local non-government organizations across the nation. Centers are geared specifically to provide training for women in finance, management, marketing, procurement and the Internet.

For more information about SBA business development programs and services call the SBA Small Business Answer Desk at 1-800-U-ASK-SBA (827-5722) or visit our website, www.sba.gov.

Other U.S. Government Resources

Many publications on business management and other related topics are available from the Government Printing Office (GPO). GPO bookstores are located in 24 major cities and are listed in the Yellow Pages under the bookstore heading. Find a "Catalog of Government Publications at http://catalog.gpo.gov/F

Many federal agencies offer Websites and publications of interest to small businesses. There is a nominal fee for some, but most are free. Below is a selected list of government agencies that provide publications and other services targeted to small businesses. To get their publications, contact the regional offices listed in the telephone directory or write to the addresses below:

Federal Citizen Information Center (FCIC)
Http://www.pueblo.gsa.gov
1-800-333-4636
The CIO offers a consumer information catalog of federal publications.

Consumer Product Safety Commission (CPSC)
Publications Request
Washington, DC 20207
http://www.cpsc.gov/cpscpub/pubs/pub_idx.html
The CPSC offers guidelines for product safety requirements.

U.S. Department of Agriculture (USDA)
12th Street and Independence Avenue, SW
Washington, DC 20250
http://www.usda.gov
The USDA offers publications on selling to the USDA. Publications and programs on entrepreneurship are also available through county extension offices nationwide.

U.S. Department of Commerce (DOC)
Office of Business Liaison
14th Street and Constitution Avenue, NW
Washington, DC 20230
http://www.osec.doc.gov/obl/
DOC's Business Liaison Center provides listings of business opportunities available in the federal government. This service also will refer businesses to different programs and services in the DOC and other federal agencies.

U.S. Department of Health and Human Services (HHS)
Substance Abuse and Mental Health Services Administration

1 Choke Cherry Road
Rockville, MD 20857
http://www.workplace.samhsa.gov
Helpline: 1-800-workplace. Provides information on Employee Assistance Programs Drug, Alcohol and other Substance Abuse.

U.S. Department of Labor (DOL)
Employment Standards Administration
200 Constitution Avenue, NW
Washington, DC 20210
The DOL offers publications on compliance with labor laws.

U.S. Department of Treasury
Internal Revenue Service (IRS)
1500 Pennsylvania Avenue NW
Washington DC 20230
http://www.irs.gov/business/index.html
The IRS offers information on tax requirements for small businesses.

U.S. Environmental Protection Agency (EPA)
Small Business Ombudsman
1200 Pennsylvania Avenue NW
Washington, DC 20480
http://epa.gov/sbo
Hotline: 1-800-368-5888
The EPA offers more than 100 publications designed to help small businesses understand how they can comply with EPA regulations.

U.S. Food and Drug Administration (FDA)
5600 Fishers Lane
Rockville MD 20857-0001
http://www.fda.gov
Hotline: 1-888-463-6332
The FDA offers information on packaging and labeling requirements for food and food-related products.

For More Information

A librarian can help you locate the specific information you need in reference books. Most libraries have a variety of directories, indexes and encyclopedias that cover many business topics. They also have other resources, such as

- **Trade association information**
  Ask the librarian to show you a directory of trade associations. Associations provide a valuable network of resources to their members through publications and services such as newsletters, conferences and seminars.

- **Books**
  Many guidebooks, textbooks and manuals on small business are published annually. To find the names of books not in your local library check Books In Print, a directory of books currently available from publishers.

- **Magazine and newspaper articles**
  Business and professional magazines provide information that is more current than that found in books and textbooks. There are a number of indexes to help you find specific articles in periodicals.

- **Internet Search Engines**

In addition to books and magazines, many libraries offer free workshops, free access to computers and the Internet, lend skill-building tapes and have catalogues and brochures describing continuing education opportunities.