

A risk management guide to protect your business against crime
Don't take chances



Contents

- 1 Introduction
- 2 Management's role
- 5 Embezzlement
- 10 Computer crime
- 13 Employee theft
- 15 Shoplifting, burglary and robbery
- 20 Additional protection

Published by

Zurich Services Corporation

1400 American Lane

Schaumburg, Illinois 60196-1056

Introduction

Business leaders pride themselves on knowing what's going on in their product lines and markets. They spot opportunities early and know how to handle competition. They know how to organize their businesses and operate efficiently. Good managers have the foresight and insight to handle just about every business situation.

Yet in all the planning and consideration of contingencies, some of the most common threats to a business' reputation and profit are often overlooked. Because the risk seems insignificant, because the likelihood seems remote, because people would rather not deal with it — for whatever reason — some business owners and managers never fully consider the possibility of embezzlement and theft and the appropriate preventative measures.

The fact is that crime is a significant cost of business. Embezzlement and employee theft is far more common in virtually all types of business than most people realize. Current estimates indicate that these dishonest activities cost American firms around \$400 billion a year. The nightly news and crime statistics bear out the frequency and additional cost to business of shoplifting, burglary and robbery.

How do you protect against crime? While no foolproof security against employee dishonesty or other criminal acts exists, you can significantly reduce the risk to your business. Sound management minimizes loss, and prevention is the best protection.

This booklet is designed to help you prevent losses from dishonest acts, particularly those committed "on the inside" by employees. It identifies ways to avoid circumstances that increase the opportunity for embezzlement and theft. It does not cover all possible situations, and there is no way to guarantee that the measures described will succeed in all instances.

Given the opportunity and motivation, some people will resort to criminal behavior. However, you can reduce the risk by understanding the reasonable measures suggested in this booklet for safeguarding your business.

Management's role

The first step to encouraging high ethical standards is creating a culture of integrity and professionalism. Best practices suggest focusing on the following:

Management integrity

Set the highest standards for yourself, and abide by them. When you conduct your business with integrity, you send the message to employees that honesty is expected. Never dip into petty cash, cash receipts or accounts for personal spending money, even for a temporary advance. Careless regard for the company's assets will be recognized quickly, and in many cases, employees will adopt the behavior. Employees who see their managers adhering to high ethical standards are likely to follow their example.

Employee selection

Screen and select employees carefully. The level of screening should vary depending upon the needs of your company and the security required in each position. A conscientious reference check on every new employee is one of the most important security measures you can employ. Remember that a hiring mistake could be a drain on your company's profits for months or years to come and result in irreparable damage to other employees and customers.

You may want to verify employment history, scholastic achievement, and possible criminal history of a prospective or new employee by contacting former employers, references and credit bureaus or similar agencies. Require an explanation for missing time periods. Keep in mind that the rights of individuals must be preserved when receiving, furnishing and using background information. Also, make sure that no one is placed on the payroll without proper authorization, and have your personnel department periodically check additions to and deductions from the payroll.

Other tools that may be useful are credit checks, psychological tests, polygraph tests where allowed by law and personal character examinations. When appropriate and for particularly sensitive jobs, a review of public records and filings might be warranted.

Employee treatment

Treat employees fairly and with dignity. Train and equip employees to accomplish tasks. Make sure that hours are reasonable, breaks are assigned, and restroom and break areas are clean and attractive. Set reasonable work rules and apply guidelines consistently. Make sure that lines of responsibility and authority are clearly understood and that employees are rewarded for outstanding performance. Make sure no employee is irreplaceable. Make sure employees take vacation. Cross training and rotation of duties is important and provides an excellent opportunity to review the work of key employees. Finally, learn as much as you can about your employees. You or a co-worker may be the first to detect unusual behavior that may indicate drug addiction or other disorders. Be aware of extraordinary circumstances such as employees who are always early to work and the last to leave, illness that creates a financial drain, family problems that might present a financial strain (divorce or abuse), or an employee clearly living beyond their means. Historically, these behaviors have been associated with the reasons for embezzlement and theft.

Performance standards

Adopt a standard of excellence in conduct and performance. Encourage your employees to be the best and take pride in their jobs. People who feel pride in their work accept responsibility for their performance. Set a zero-shortage goal as a standard of excellence. Even if pilferage falls to a minimum level, the constant effort to reach the zero-shortage goal should be maintained.

Create a code of ethics

Define in writing what standards are expected. These standards should discuss issues such as relationships with customers and vendors and conflict of interest issues. A policy on receipt of gifts from vendors and customers should be included. There should be a no tolerance policy pertaining to dishonest behavior. Proof of dishonesty should result in immediate termination of employment. Additionally, if theft or embezzlement is proven, experts recommend filing criminal charges. This will demonstrate to your other employees your commitment to not tolerating dishonest behavior and possibly discourage future thefts. Remember, the thief or embezzler is the "bad guy," not you. By knowingly allowing a dishonest

employee to continue in your employ, you may jeopardize your fidelity insurance coverage, placing your company at greater risk of monetary loss.

Hotlines

If an employee is engaged in dishonest conduct, often others are aware of the activity but are frightened to reveal the behavior. One solution is an anonymous hotline where employees can report improprieties. BE CAREFUL, do not make allegations against an employee unless there is independent corroboration of the facts.

Get help!

When you suspect theft or embezzlement, contact the police or a professional security consultant for help. Don't try to solve the crime on your own. You could hinder the investigation and destroy evidence or jeopardized key documentation or testimony. Also, you could risk exposing your company, your co-workers and yourself to liability or serious danger. Cooperate with the authorities, and keep your bonding company informed. Remember, your bonding company will need conclusive proof of both the theft or embezzlement and the amount missing to help you recover your losses.

Fidelity bond

Make sure that employees are bonded. They might think twice if they know that a bonding company also has an interest in their actions. Communicate the fact that the practice of bonding employees is a company policy, not an indication of mistrust.

Embezzlement

Embezzlement happens when you trust an employee with your business assets, and the employee takes your property. Embezzlement is theft with the distinction of happening “on the inside.”

Embezzlers resort to all kinds of ploys to steal from businesses. They pocket cash by issuing checks to pay phony or duplicate bills. They accept kickbacks from customers for unauthorized discounts, take cash on sales while not recording them and keep money collected on “uncollectible” accounts. Some schemes are more elaborate. With the aid of technology, data can be altered and funds transferred in a matter of seconds. Forged checks can be destroyed after they clear the bank. By applying subsequent payments against shortages, embezzlers can cover small amounts taken from payments. Payrolls can be padded. Cash can be taken from the register while altering the tape, and cash can disappear by charging amounts to fictitious customers. In short, wherever a transaction can be interrupted or duplicated by an employee, embezzlement can occur.

Embezzlement is fraud perpetrated by someone you employ and trust, and it is the trust that creates the opportunity for embezzlement. There is no simple way to prevent embezzlement, because businesses require some degree of trust to operate. In fact, some of the largest, most successful firms have high levels of trust and many “empowered” employees. But they also follow sound management practices and have effective internal controls.

While there is no single solution for embezzlement, some standard business practices are recommended for the prevention and detection of this type of fraud.

Accounting controls

Use an accounting system designed to track revenue and expenses for your type of business. Consult a qualified public accountant for assistance in establishing, analyzing and improving your business's record keeping. Test the accounting controls thoroughly. Check for weaknesses an embezzler could exploit, and audit the books annually. Pay particular attention to payroll tax payments and employee benefit guidelines.

Cash registers/point of sale terminals

If cash registers are used, assign each clerk their own register if possible; otherwise, limit the number of people per shift assigned to each register. Clear the registers frequently—at least twice daily—of cash in excess of the amount needed for change and balance the amount of cash and the sales recorded by each register. Registers should be cleared and checked by supervisors. Review voided transactions or frequent “overrides.” Verify with cash register manufacturer that the register cannot be operated while off-line or in print only mode. Point of sale (POS) terminals perform many additional functions as compared to cash registers and therefore can place you at greater risk because of its ability to handle credit/debit card transactions and maintain perpetual inventory.

Sales records

If pre-numbered sales receipts are used to record sales, make each sales person accountable for the tickets in their pads. Use tickets that automatically make copies so that matching receipts are produced for customers and your records. Randomly review receipts to ensure that there are no missing or duplicate numbers. At the close of business each day, balance cash received by the cashier and the total amount of the sales tickets.

Cash collection records

Divide duties so that no single employee is responsible for both receiving cash and recording collections in your business's accounts receivable records. If cash is routinely received in your business, give numbered, signed receipts to all persons from whom you receive cash. The collection clerk should list cash and checks received, note the amount and source of each transaction, then sign the list when cash and checks are turned over to the company cashier. The cashier should stamp all checks “for deposit only,” deposit the funds, sign the list and send a copy to the accounting department. Deposit all checks within 24 hours of receipt, and obtain duplicate deposit slips or other documentation from the bank. Check cash receipt records daily to make sure that collections match deposits. Someone other than the person who prepares deposits and withdrawals the funds should reconcile bank statements. Again, the key is to separate cash handling and recording duties, and make sure that the cashier and the

bookkeeper are unable to alter the other person's records. Establish similar controls for approving unusual discounts and bad-debt write-offs.

Cash disbursement records

Delegate check signing and cash disbursement authority very carefully. Divide the duties of payroll preparation and payroll disbursement among different people, especially when cash is involved. Minimize cash disbursement activity, and only approve payments with sufficient documentation or prior knowledge of each transaction. Examine all invoices to confirm receipt of merchandise, and verify prices before signing checks. Cancel all invoices when checks are signed so they cannot be resubmitted for payment. Use serially numbered checks for all disbursements, including purchases and payrolls. Verify that your automated check writing system will not print duplicate checks or multiple checks with the same check number. Generate checks electronically, or write them in ink on safety paper. Inspect pre-numbered checkbooks occasionally to make sure that checks from the back of the books are not missing. Require countersignatures on checks, and limit the authority to countersign. Don't sign blank checks, and don't leave a supply of blank checks for any reason. Examine cancelled checks and endorsements for irregularities. Additionally, carefully review voided checks and the reasons given for the voided transaction. Bank statements should be reviewed for any irregularities. A person other than the one who does reconciliation should review bank statements for unauthorized endorsements by employees, endorsements by unknown parties or unfamiliar vendors.

Petty cash procedures

Establish a specific fund with a low dollar limit to cover normal daily cash requirements. Do not mix petty cash and other cash. Require a written request for a petty cash withdrawal along with a supporting voucher or sales receipt plus the signature of an authorized supervisor of the person receiving the cash. Cancel vouchers to prevent reuse, and replenish the fund by drawing a check in the amount of the vouchers. Record daily use of the petty cash fund in the general edger. Have someone other than the petty cash supervisor check the fund and balance the records. Conduct frequent, unannounced audits of the petty cash fund to guard against petty embezzlements and discourage

unauthorized cash advances. Do not allow customer or vendor cash to be commingled with petty cash. Also, avoid using petty cash as a way of reimbursing employee expenses since this allows the employee expense account safeguards to be by-passed or duplicated.

Cash/funds transfers

Divide authority for transfers between accountants so that no one person or same group of people can transfer funds within your organization.

Mail

Have the company mail sent to a post office box rather than your place of business, and control who opens the mail and lists cash and checks received. If warranted, a second person should be involved in the process as a guard against impropriety. Have the lists and checks double-checked by someone other than the person compiling the original list. Arrange for bank statements and other bank correspondence to be sent to the post office box.

Vigilance

Pay attention to preventing opportunities for embezzlement. Check your internal controls frequently, and look for signs of trouble, such as:

- An increase in the amount or frequency of refunds for returned merchandise. Items might be defective, or the refunds could be a cover for someone stealing from accounts receivable
- Unusual bad-debt write-offs or unusually slow collections. Business conditions might be poor, and your customers might not be able to pay. However, they could be paying, while a dishonest employee is pocketing the funds
- A decline in revenue. Business might be off. Then again, business could be fine, but sales are not being recorded
- Inventory shortages. Stock may have been miscounted or misplaced. Or an actual level of inventory below the recorded level could indicate unrecorded sales, fictitious purchases or employee pilferage. Verify your inventory on a regular basis; and
- A profit decline or expense increase. Costs do rise, but sometimes the additional expense signals that cash has been misappropriated.

In summary, the risk of embezzlement can be reduced by instituting strong accounting controls, separating cash handling and recording duties, checking new employees' backgrounds, bonding employees, setting an honest example and watching for signs of trouble.

If you suspect that your business has been the victim of embezzlement, proceed with caution. What appears to be misappropriation of funds or property could have a plausible explanation. A false accusation could expose you and your company to civil liability. Also, you could lose the services of a valued employee and irreparably damage the good reputation of a colleague.

If you believe that embezzlement has occurred, contact your attorney and be guided by legal advice. Discuss the necessity of notifying the appropriate law enforcement authorities and your bonding company. If the evidence is sufficient, experts recommend criminal prosecution of the embezzler. Don't help conceal the commission of a crime and risk sending the message to other employees that dishonesty will be tolerated under some circumstances. Again, your attorney will be best qualified to advise you on how to proceed.

Computer crime

Computer-assisted fraud almost seems exciting. It's new. It's complex. It pits the clever computer wizard against the big, established computer-run company. In fact, this sense of adventure does attract some people to this form of crime and certainly gets lots of publicity. However, the truth of the matter is that computer-assisted fraud is a crime—no different than embezzlement and in some ways a more serious threat to the assets of the company and to the privacy of its workers, suppliers and customers.

Despite the popular image, computer crime is not typically glamorous. Quite often, a dishonest employee with relatively little technical knowledge commits it or it can be the successful hacker (outside the premises). The computer merely provides access to records and the opportunity for crime—no different than altering written accounts with a pencil.

Most of the keys to preventing computer crime are similar to other safeguards against embezzlement. Here are a few more:

Documentation

Document procedures in writing for systems development, maintenance and security. Test the procedures and update the documentation regularly.

Physical security

Secure data processing facilities by using locks, security guards, badges, access cards, electronic controls, access codes and passwords. Secure remote terminals, personal computers and communications lines, especially those connected to networks. Have a "firewall" in your system to help prevent unauthorized access by remote users.

Security policies

Communicate clearly your company policies to all employees for data access, security standards, security codes and security violations. Periodically revise security codes and immediately delete codes of terminated employees. Insist that passwords be changed frequently and kept confidential by employees. Make it known that employee activity can and will be periodically and randomly monitored. Make sure that computer access and authorizations are immediately withdrawn upon termination of an employee.

Restricted access

Limit who has access to system files and documentation, and track access with user logs. Control and monitor access to confidential data. Incorporate features in systems to identify repeated attempts to gain access. Log-off users after periods of inactivity or after repeated unsuccessful attempts to gain access to restricted information.

Back-up

Regularly back up software and data files so that information can be recovered when data is lost, damaged, contaminated or altered, intentionally or unintentionally. Alternate personnel responsible for doing the back-up.

Rejected transactions

Correct rejected transactions on a timely basis to limit the exposure to transactions circumventing normal processes and controls. When establishing a work-around include review and audit of the new procedures.

Master file transactions

Assign someone who is not involved in routine data processing to reconcile critical master file transactions with documentation so that all file changes are authorized.

Separate duties

Where possible, segregate the tasks of developing systems from the jobs that involve using the systems. Control access to specific accounts by restricting it to individuals outside the data processing department. Systems people should not be involved in addressing customer or supplier account discrepancies. Segregate the identification of errors and reconciliation of batch control totals from systems applications.

Management

Apply the same sort of careful planning, organizing, staffing and controlling skills to your data processing operation as you would to any other area. Realize that access to computers is no different than access to the books and files of your business. If anything, it is broader in scope, faster to exploit and potentially far more dangerous. The need for effective management and appropriate controls is apparent.

Get smart

The more you know about your computer and its security safeguards the better. You don't have to be the "expert" just be a conscientious informed user. If you suspect or detect computer-assisted fraud, act quickly. Contact the authorities immediately. Rely on the experts and follow the same precautions you would for handling embezzlement or theft. Remember to persevere if the authorities indicate prosecution is warranted.

Employee Theft

Most employees don't steal, but some do. Many of your employees would never take cash from another business' register or shoplift from another establishment. An asset of your business, however, might be seen as a job benefit or something so insignificant that it will never be missed. The sad fact is that dishonest employees account for two-thirds of theft.

Employee theft ranges from pilfering pens and pencils to grand larceny of equipment or finished goods. Methods vary, too. Items are slipped into pockets, pocketbooks or briefcases with little or no forethought. Or someone might plan ahead, hide when the business closes, then carry out the theft in solitude. In any case, the action constitutes theft. Stealing is stealing. It is a cost of business that robs from the potential funds available to cover other costs, including the wages and salaries of all employees as well as the profit of the company.

There is no certain way to avoid employee theft, but there are recommended steps to reduce the opportunity and risk.

Return and refund duties

Assign a supervisor to inspect and verify the receipt of returned merchandise either as a means of double-checking refunds or before authorizing refunds made by the salesperson or cashier.

Shipping/receiving and recording duties

Require the completion of receiving reports as soon as items are received, then conduct a second check of materials to verify quantities logged in by employees who handle receiving. Make sure that supervised shipping personnel, not drivers, load trucks.

Trash disposal

Supervise trash pickups, and occasionally check trash collection sites and trucks. Collusion between dishonest employees and haulers is not uncommon. Also, don't accumulate trash or have it picked up near where valuable materials are stored.

Physical security

Use key controls, time locks, security access codes, alarms, and security guards to discourage dishonest employees. For maximum protection, limit the number of active doors. Change keys when employees leave and on a periodic basis. When shipments are received or shipped, station a supervisor or security guard at the door or loading dock as long as the door remains open. A central station alarm can be effective in protecting your company after hours. Instruct guards to investigate all unexpected door openings and notify police of suspicious activity. Likewise, time locks can be used to record all opening of doors.

Motion detectors, surveillance cameras, electronic eyes and central station alarms can be effective in preventing “break outs.” This type of theft occurs when someone, often an employee, conceals himself in your establishment until after hours, removes property, then closes the door behind him, leaving no evidence of intrusion.

Internal controls

Take physical inventory at regular intervals—monthly, semi-annually or annually, depending on the type of business concerned. With the advent of bar-coded inventory controls and programmable cash registers, it is possible to maintain a perpetual inventory. Spot-check inventory records at random to detect and discourage shortages. Assign inventory checking to people other than the employees who normally work in the inventory storage area. Conduct unannounced inspections of work areas, warehouses, storerooms and loading docks at frequent and random intervals. Also, a method some owners and managers find effective is to commit deliberate errors to gauge the effectiveness of internal controls; they then monitor the error, discover when and where it is caught, and evaluate how employees handle it.

Shoplifting, burglary and robbery

Shoplifting, burglary and robbery represent criminal threats to your business “from the outside.” They are not typically committed by employees, so internal controls alone are inadequate for their prevention and detection. Be aware however, that employees may work in collusion with an outsider. These crimes are mentioned briefly with the advice that you should consult the security experts in your industry for more information and appropriate safeguards.

Shoplifting

Shoplifters defy the demographics. They come in all sizes, races and ages. They resemble your customers. In fact, they are your customers with the one difference being that while they take possession of your goods, they choose not to pay. Juvenile shoplifters sometimes work alone on a dare or enter shops in gangs to intimidate people. Impulse shoplifters don't plan, they just give in to temptation and take advantage of sudden opportunities to steal. Alcohol, drugs or desperate circumstances can motivate shoplifters. Kleptomaniacs are driven to shoplift by psychological needs. Other shoplifters are highly skilled and hard-to-detect professionals. They use bulky items, large bags and loose clothes to conceal items, and they prefer to “work” when your store is least busy and has the lightest staff on duty.

Ways to prevent or minimize shoplifting include:

Employee awareness

Teach your employees to look out for concealment devices and group shoplifting tactics in which one person diverts the sales person's attention while another person steals, customers who shop only when staff is low, or customers who linger in one area. Instruct sales people to offer assistance; customers like attention, but shoplifters don't.

Visibility

Make it easy for your employees to monitor activity. Maintain adequate lighting. Keep displays low, well spaced and neat. Encourage employees to “circulate” through the store and avoid being stuck behind the counter or on the telephone.

Physical security

Place entrances and exits where they can be monitored. Place height guides at each door. Block unused checkout counters. Use surveillance devices—anything from mirrors to cameras, depending on your security needs. Employ uniformed guards if necessary. Place valuable merchandise behind counters or in locked displays. Use electronic tags removed by cashiers, and make sure that receipts are stapled to the outside of packages.

Discuss how to handle shoplifting with your local police. States have different laws regarding the apprehension of shoplifters. In general, to charge someone with shoplifting, you or your employees must be able to see the person steal or conceal an item, testify that it was taken with the intent to steal, identify the item as yours and prove that it was not purchased. Also, sales people and cashiers should not attempt to apprehend shoplifters; instead, they should alert managers, security personnel or police. You and your employees should avoid confronting someone with an accusation of shoplifting. The better way to handle a suspected shoplifter is to indicate that they might have merchandise that they forgot to pay for. Then ask if they can come with you to straighten out the matter. Due to the risk of false arrest or unnecessary physical contact, you should consult the experts, including your local authorities, on how to handle shoplifters.

Burglary

While shoplifters work when the store is open, burglars strike when the business is closed. Burglary entails unlawful entry to commit a theft or felony. It happens with great frequency, and because witnesses are rare and evidence is thin, burglars are caught only one in five times.

The key to controlling burglary losses is to discourage the burglar. Make your business unattractive to someone considering unlawful entry. Prevention of burglary depends on physical security measures.

Doors and windows

Talk to a locksmith and install pin-tumbler cylinder locks, deadbolt locks or other appropriate locking devices on all exterior doors. Use bars, especially on rear doors. Issue keys only as needed, keep distribution records current, avoid opportunities for others to duplicate keys, use codes to identify keys rather than

labels, and periodically check the key inventory. In windows, use burglary-resistant glass and install heavy metal screens where possible. Remember to change locks when keys are lost or disappear, when suspicious activity is discovered, or an employee who formerly had keys is no longer employed.

Alarms

Silent central-station alarm systems are the most effective alarms, because they alert the authorities not the burglar. Where these systems are not available or practical, use a building alarm. Apprehension of the burglar is less likely, but the burglary can be interrupted.

Lighting

Place outdoor lighting on all sides of buildings to deny burglars the cover of darkness. Leave indoor lights on so police or security personnel can see in. When lights are off, the burglar has the advantage of being able to see out while police cannot see in.

Safe

Use a safe strong enough to deter burglars, and keep cash in a burglary-resistant money chest. The safe should be located in well-lighted and visible area, not tucked away in a low visibility area. The safe should be bolted to the building. Also, deposit your excess cash in the bank daily. Overnight, keep only the minimum amount needed to start your business the next day.

Private security

Supplement public protection with private police. Regular patrols discourage burglars and can help detect and handle burglaries. Also, watchdogs offered by private agencies can be effective deterrents to both burglars and vandals.

If a burglary occurs, notify the authorities immediately. To preserve evidence, keep the business closed until police arrive. Afterwards, review your security measures and modify them to prevent future burglaries.

Robbery

Robbery is a violent crime in which theft is achieved through force or the threat of force against a person. More than half a million robberies occur in the U.S. each year. Two-thirds of them involve weapons. Only one-third end in arrest, and very few result in the recovery of stolen cash or property.

The prevention and handling of robberies is particularly important since lives as well as property are often at risk. Work with your local authorities and professional security consultants to avoid robbery and to prepare thoroughly for what to do if it occurs.

Robbers want to get in and get out quickly and unobserved, and they prefer to strike when the payoff is highest and their risk is lowest. Deterring robbery entails many of the security measures mentioned for shoplifting and burglary. Additional steps for avoiding and handling robberies are suggested.

Cash

During business hours, remove excess cash from the primary area of exposure, and store excess cash in a locked safe. Also, deposit cash in the bank to keep it away from the business premises. Use an armored car service, or take cash to the bank at different times by different routes each day. Keep duplicate copies of deposit slips, checks, etc. on site to expedite documentation of any loss. You will also want to notify any customers immediately if their checks have been stolen to mitigate your damages.

Opening and closing routines

Use two people to open or close the business—one inside to inspect the premises and deactivate or activate the alarm, and one person outside who observes their partner and is prepared to use the nearest phone to contact the police if a robbery is suspected. Also, be wary of night calls for emergency repairs or other excuses that would bring you or an employee to the business with keys to open it. Call the police if the burglar alarm breaks, and verify all after-hours service calls. If two people cannot open and close your business, insist that the person call in and report proper, safe opening. Have a plan or password to alert the person called there is trouble.

If a robbery occurs, remain calm. The first priority is to protect people, not by being a hero but by keeping quiet, listening to the robber's instructions, and following them. The potential for violence is too great to risk intervention. Instead, simply cooperate. Activating silent alarms, memorizing descriptions and noting the direction of escape are worthwhile activities but only if they can be done without increasing the potential for harm.

After a robbery, lock the doors, call the police, keep people calm, secure other valuables, safeguard evidence and wait for the police. Witnesses should not discuss the robbery until their recollections are written down or disclosed to the police. Also, amounts stolen and witness information should not be disclosed to the press. Don't make your business an inviting target for a return visit by a robber.

Additional protection

Strong management guided by security experts and effective internal controls can provide the best defense against crime. Yet not even the most extensive preventive measures are foolproof. Dishonest acts can and will occur.

An important part of any program to safeguard against embezzlement and theft is sufficient insurance coverage. A commercial crime policy can cover loss resulting directly from dishonest or fraudulent acts committed by an employee acting alone or in collusion with others. In addition to these fidelity features, the policy can cover the loss of property resulting directly from robbery, burglary, misplacement, mysterious disappearance, damage or destruction.

Consult your independent agent or broker regarding fidelity and crime protection for your business.

Zurich Services Corporation

1400 American Lane, Schaumburg, Illinois 60196-1056
800 982 5964 www.zurichservices.com



ISO 9001:2000

Quality-Assured Solutions Provider

The information in this publication was compiled by Zurich from sources believed to be reliable. Zurich Risk Engineering is a unit of Zurich Services Corporation. We make no guarantee of results and assumes no liability in connection with the information, methods or safety suggestions contained herein. Moreover, Zurich reminds you that this publication cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be required by abnormal or unusual circumstances.

©2006 Zurich Services Corporation

