TOTAL ASSET PROTECTION

A BUSINESS OWNER'S GUIDE TO PREVENTING INTERNAL THEFT

Prepared by:
THE GOVERNOR'S EXECUTIVE ADVISORY COUNCIL
Marshall M. Meyer, Chairman

TOTAL ASSET PROTECTION

A BUSINESS OWNER'S GUIDE TO PREVENTING INTERNAL THEFT

Prepared by:
THE GOVERNOR'S EXECUTIVE ADVISORY COUNCIL
Marshall M. Meyer, Chairman

IN COOPERATION WITH THE MARYLAND
DEPARTMENT OF ECONOMIC & EMPLOYMENT DEVELOPMENT
Mark L. Wasserman, Secretary

IMPACT OF CRIME ON BUSINESS IN MARYLAND TASK FORCE
Frank J. Napfel, Co-chairman
Kai R. Martensen, Co-chairman

SPONSORED IN PART BY THE
SMALL BUSINESS CENTER DEVELOPMENT NETWORK

December, 1994

"THE MORE PEOPLE WHO OWN LITTLE BUSINESSES OF THEIR OWN,
THE SAFER OUR COUNTRY WILL BE,
AND THE BETTER OFF ITS CITIES AND TOWNS;
FOR THE PEOPLE WHO HAVE A STAKE IN THEIR COUNTRY
AND THEIR COMMUNITIES
ARE ITS BEST CITIZENS."

- - JOHN HANCOCK

STATE OF MARYLAND
OFFICE OF THE GOVERNOR

WILLIAM DONALD SCHAEFER
GOVERNOR

Dear Business Person:

As I read the quote by John Hancock, I realize how fundamental our small businesses have always been to the economic fabric of our society, and to the values we honor. This is even more apparent today, as our economy becomes more diverse, and many of our former corporate giants find themselves "right-sizing" and looking outside the corporate structure to accomplish functions formally handled internally. The entrepreneurial spirit that fosters the growth of small businesses has always contributed to new job opportunities. Obviously, our economic future will be bleak if this core sector of our economy is not encouraged to continue the rapid growth it has enjoyed over the last decade.

I am deeply concerned that many published surveys reveal that many small companies do not survive the first five years. Although these businesses fail for a variety of reasons, it is well documented that a third fail because of losses caused by diversion of assets, commonly termed internal theft. This deviant behavior actually encompasses many other damaging activities.

We have support systems to help small and medium size business owners cope with many traditional business problems, such as the Small Business Development Center and other programs offered by the Department of Employment and Economic Development. Until now, however, there has not existed in Maryland a source of information for small businesses facing the threat of internal loss.

I have asked that this important publication address those internal security issues often faced by small to medium-sized businesses who do not have a security professional on staff. It is my hope that a careful review of this material and its continued use as a reference guide will help Maryland's businesses prevent internal security problems, and will serve as a blueprint for responding to these problems when they do occur.

It is my personal commitment to provide a positive environment for the creation and growth of all businesses in Maryland. I hope this publication will be a valuable tool in producing that environment for you and the success of your business .

Sincerely,

William Donald Schaefer

Governor

PREFACE

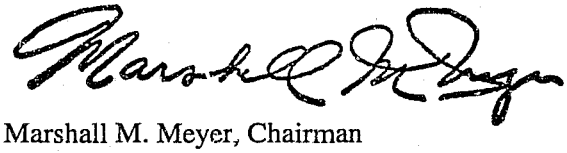
When this project was initiated many months ago, it was thought we would merely gather statistics regarding the incidence of various offenses and then issue a report concerning the impact this crime had on small- and medium-sized businesses. Though we quickly recognized the need to accumulate relevant statistics, it became apparent that we would need specialized information from various "expert" sources. At the same time, we also initiated a review of available literature and decided to concentrate most of our efforts at examining the causes of internal corporate losses.

We found that while there were numerous textbooks dealing with the issue of internal theft, there were very few practical guides for the small- and medium-sized business owner. The few notable exceptions have been cited as reference material within this *Guide.*

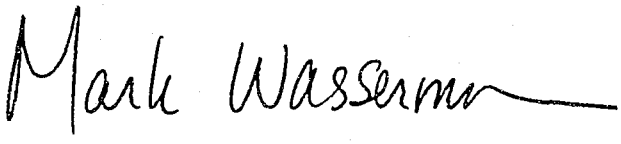
In the hope of providing practical information, we embarked on an effort to produce a *Guide* that both the novice and professional could utilize in planning a comprehensive security program for any size company. We have attempted to outline simple concepts, based on the principle of prevention, that can enhance an existing program or serve as the foundation for a total loss prevention program.

Our degree of success will be measured by our ability to keep you interested and by the untold thousands of dollars in losses that will be prevented. You can be assured that every recommendation or suggestion in this *Guide* has been reviewed by leading members of the Bar and nationally recognized security professionals.

I would like to especially thank Governor William Donald Schaefer who recognized the importance of this *Guide* and authorized its publication. I also want to thank Secretary Mark Wasserman and the State Department of Economic and Employment Development for their distribution of this publication.



Marshall M. Meyer, Chairman
Governor's Executive Advisory Council



Mark L. Wasserman
Secretary
Department of Economic and Employment Development

Table of Contents

List Of Figures

List Of Summary Boxes

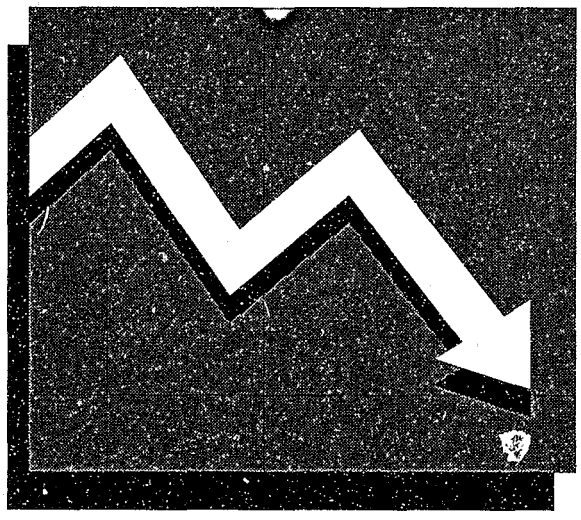
INTRODUCTION

Have you ever asked yourself any of these questions or faced any of these problems?

- *"Three weeks ago, I caught an employee stealing, obtained a verbal confession, and arranged for his/her restitution to my company. I then fired the employee. I have not received any restitution to date—what can I do?"*
- *"My business has been plagued by a recent rash of bad checks accepted by my employees. How can I stop this?"*
- *"I have several employees exhibiting strange behavior before drug tests, but they all tested negative!"*
- *"I have received several anonymous calls warning me that company products are being sold 'on the street,' outside of normal channels."*

This task force was empowered to help you address these questions by developing a comprehensive *Guide* that smaller business owners can use to create a business environment protective of company assets. Your company's assets.

WHY SHOULD YOU BE CONCERNED ABOUT CRIME?



Crime impacts your bottom line!

Each year, all sectors of business—retailing, manufacturing, wholesaling, services, transportation, etc.—lose billions of dollars to crime. We tend, in an entrepreneurial haste to "grow the business," to immerse ourselves in day-to-day business routines and often ignore the protection of our assets. Ironically, small- and medium-sized retailers lose three times more in receipts than their larger counterparts, a proportionally far greater loss because they are less able to absorb loss or to afford extensive protection.

We want to emphasize that all criminal threats are not external. "Only under extreme duress (do) business owners... turn inward to pinpoint sources of losses," notes one consultant. When you fail to tighten internal security controls, you open yourself to "the enemy within"—all potentially dishonest employees. Employee theft accounts for the majority of business dollars lost to crime: an estimated 30% of all business failures are directly attributable to theft by employees unaware that they are siphoning off profits that jeopardize their company's existence and their own jobs.

WHAT CAN YOU DO?

Our message is that **prevention** is much simpler, more efficient, and more profitable than detection, employee termination and replacement. Adopting the philosophy of prevention can help limit the dollars lost when theft occurs by ensuring that you are informed early and act quickly.

Even if you are lucky enough to receive an insurance recovery, you still will have consumed countless hours fixing a problem that probably did not have to occur. Additionally, insurance companies must, like yourself, be profitable. Eventually, you and other businesses will pay for your loss.

WHAT WILL THIS *GUIDE* DO FOR YOU?

We are presenting a fundamental course in prevention that will help you conserve the assets you are working so hard to accumulate. We don't want your company to be another statistic reflected in the list of companies that seemed to be doing so well—until a large embezzlement, theft ring, or fraud scheme drained them of assets. This scenario repeats itself thousands of times every years, and the victimized business owner is usually heard to utter one of the following phrases:

- *"I had no idea!"*
- *"He was my most trusted employee!"*
- *"Why didn't someone tell me?"*
- *"How could they do this to me?"*

"This"—employee theft—can and will happen to you, but only if you unwittingly allow it. Unmotivated **employees**, possibly prone to criminal behavior, or even trusted employees, driven by economic circumstances, **will take advantage of your failure to install preventive measures** and can damage or destroy your company.

FORMAT AND CONTENT

We have asked our experts—private security, law enforcement professionals, and seasoned businessmen—to specify in this *Guide* (in one-on-one terms) the most important prevention and security issues facing the owners of small- and medium-sized businesses. We required only that they stress those factors which **prevent** loss. Our goals are:

- to suggest areas where prevention can be designed into your own operations;
- to recommend policies that will assist your implementation of specific prevention strategies; and
- to provide you with a list of informational and service resources.

If you do not have enough time to read this *Guide* entirely, or even one chapter, we have boxes throughout the text that contain summary information of critical issues, efforts, steps-to-take, etc., that you can browse through to understand the essentials of what is more fully discussed in the text.

SAMPLE BOX

SUMMARY INFORMATION

- CRITICAL ISSUES
- KEY EFFORTS
- ESSENTIAL STEPS

Bank of America NT&SA, *Crime Prevention for Small Businesses*, 1984.

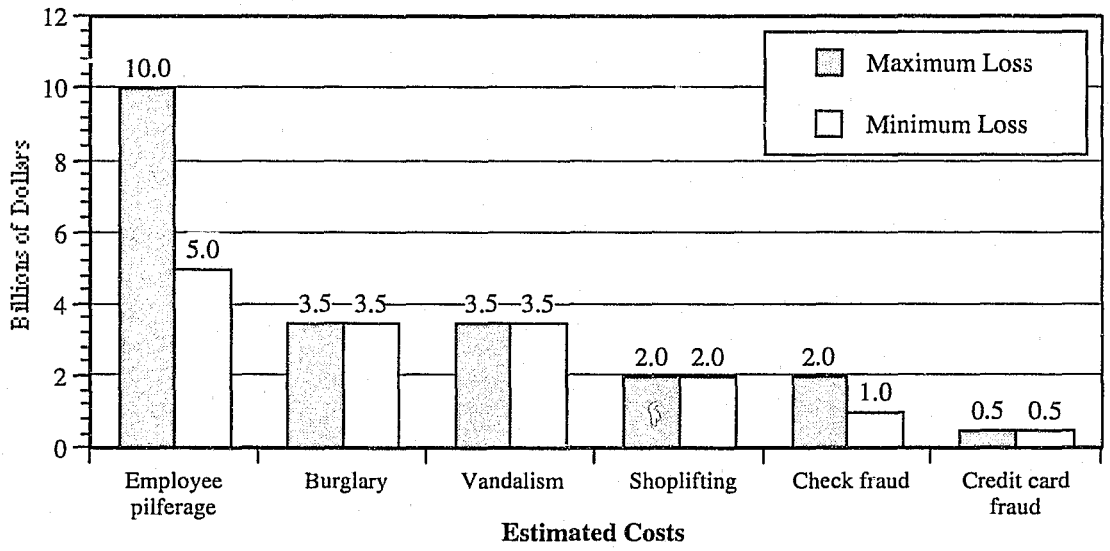
PART I. BACKGROUND AND CAUSES OF CRIME

Why Do Employees Steal From the Hand that Feeds Them?

A. BACKGROUND

Deviant employee behavior can have a more devastating effect on your business than can your victimization by burglars, robbers, or shoplifters. Your management skills are essential to forestall employee misbehavior (Figure 1).

FIGURE 1. COSTS OF NON-VIOLENT CRIMES AGAINST BUSINESS



Source: U. S. Department of Commerce, *The Cost of Crimes Against Business* (Bureau of Domestic Commerce, Domestic & International Business Administration, Washington, D.C.), 1976.

Crime Costs to Business

Business losses due to crime are estimated at $114 to $300 *billion* a year. The wide range of this sobering estimate is attributed to: differing definitions of business crimes; inadequate data bases; poor record keeping and reporting practices; and businesses reluctant to reveal financial loss data.

Crimes against business cost companies 69% of the after-tax corporate profits in America—eight times more than the costs of crimes committed against individuals and households. Consumers pay for virtually all such crime through higher prices, a "crime tax" of $1,376 per American household.

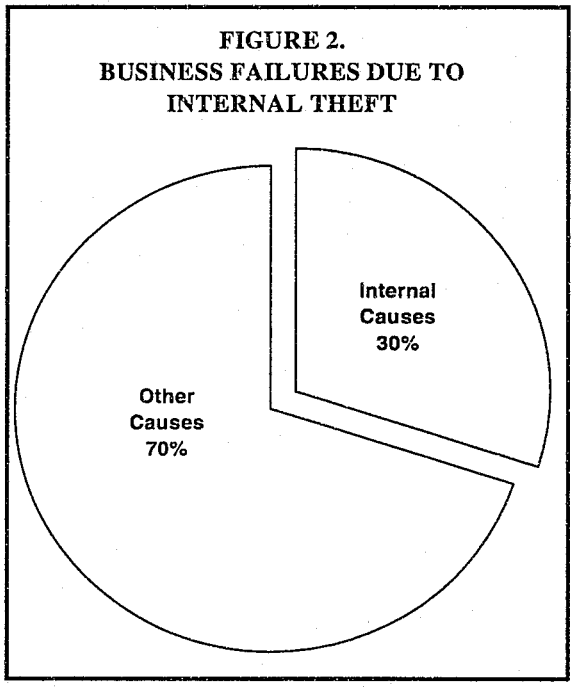
Programs and products directed at preventing crimes against businesses and diversion of company assets in America consume well over $150 billion each year. Business "insurance" (hardware and guards) against employee theft is itself a multi-billion dollar annual expense: over $1 billion is spent on locks, $2 billion on burglar alarms, and $148 billion on guards. Nationally, crime's cost to business reportedly stands at 2.3% of the GNP, and small, vulnerable sole proprietors sustain the largest share of crime losses against retail business. The U.S. Small

Business Administration reports that crime losses for businesses with receipts under $100,000 is proportionately 3.2 times the national average, and 36 times that of businesses with receipts over $5 million.

What Losses Do Employees Cause?

The American Management Association reports that the top four internal crimes affecting businesses more severely than robbery, burglary, or shoplifting—in terms of dollar loss—are employee pilferage, kickbacks/bribery, securities theft/fraud, and embezzlement.

FIGURE 2.
BUSINESS FAILURES DUE TO INTERNAL THEFT



Source: U.S. Department of Commerce, *Crimes Against Business, A Management Perspective* 1976, p. 123.

Of the estimated $12.6 billion that retailers lose to pilferage and shoplifting each year, roughly 60% stems from employee theft.

- **One-third** of employees in retail, manufacturing, and service organizations surveyed in 1983 admitted stealing from their employers.
- More recently surveyed supermarket employees admitted annual thefts averaging $143 per employee (who also believed that co-workers stole an average of $1,176 each year).
- Embezzlement and kickbacks cost businesses $27.2 billion in 1991, a figure which may be much higher due to failure to report because of corporate embarrassment or actual unawareness of deception.

Although a number of complex social and psychological factors, both in and out of the workplace, underlie the motivation(s) for employees to steal, you can do something about it.

Eleanor Chelemsky et al., *Security and the Small Business Retailer* (National Institute of Justice; formerly NILECJ), 1979.

John P. Clark and Richard C. Hollinger, *Theft by Employees in Work Organizations: Executive Summary* (National Institute of Justice), 1983.

William C. Cunningham et al., *Private Security Trends, 1970 to 2000: The Hallcrest Report II* (McLean, VA), 1990.

Richard C. Hollinger, *Dishonesty in the Workplace: A Manager's Guide to Preventing Employee Theft* (Park Ridge, IL), 1989.

John W. Jones, *Second Annual Report on Employee Theft in Supermarket Industry: 1990 Summary of Findings* (Park Ridge, IL), 1991.

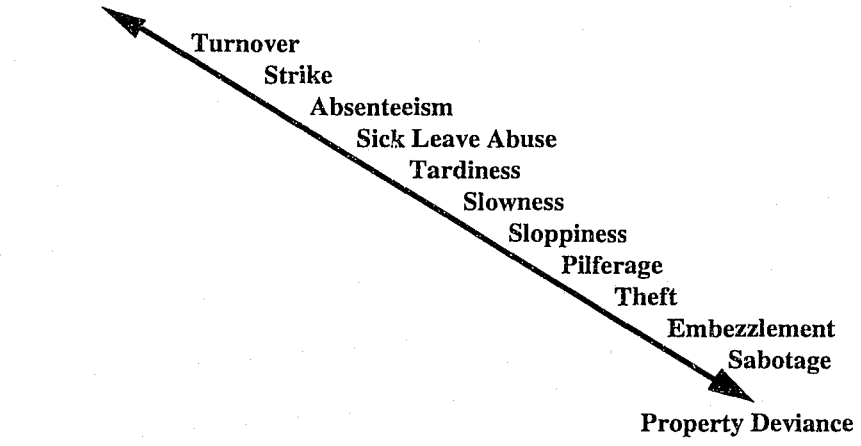
Ira M. Shepard and Robert Duston, *Thieves at Work—An Employer's Guide to Combating Workplace Dishonesty* (Bureau of National Affairs, Inc., Washington, DC), 1988.

U.S. Department of Commerce, *The Cost of Crimes Against Business* (Bureau of Domestic Commerce, Domestic & International Business Administration, Washington, DC), 1976.

B. CAUSES OF CRIME

The principal types of internal business losses are not employee theft of cash, equipment, tools, merchandise, or supplies. Those are merely overt signs that other theft, including "stealing" time, deliberately producing shoddy work, and even sabotaging your operations, may also be occurring (Figure 3).

FIGURE 3. EMPLOYEE DEVIANCE CONTINUUM



Source: Richard C. Hollinger, *Dishonesty in the Workplace: A Manager's Guide to Preventing Employee Theft,* Park Ridge, IL, 1989, p. 34.

Figure 3 represents a management problem, not necessarily a crime problem:

> "The unauthorized taking of company property, money, or any other asset by an employee is legally called theft or larceny. Since these behaviors are theoretically more similar to production deviance than to conventional street crime (e.g., burglary, robbery, etc.), it is inappropriate to view these problems in a purely legal context."

REQUIRED CONDITIONS

Experts agree that three conditions are present before a theft or other crime occurs:

Motivation to Perform the Deviant Act. This derives from one or more factors. Personal financial gain is the most "understandable" reason "why" employees embezzle. The psychological causes may be difficult to discover, and may change over time, but many employees unconsciously rationalize their acts, as in:

- *"I'm borrowing, not stealing"*
- *"Everyone else does it"*
- *"It's part of the 'perks' that go with the job"*
- *"I deserve more pay"*

Opportunity to Steal. Your own employees have more opportunity to steal than does your customer/vendor, or even a burglar/robber. You cannot eliminate the "need" to steal, but you can eliminate or reduce employee opportunities by using accepted security procedures.

Absence of Formal or Informal Controls. Your employees' belief that you are unconcerned, disorganized, or unaware will invite theft—your loss. If your employees believe nothing will happen even if they are caught, you are inviting problems.

WHY EMPLOYEES STEAL

Standard theories have been recently challenged:

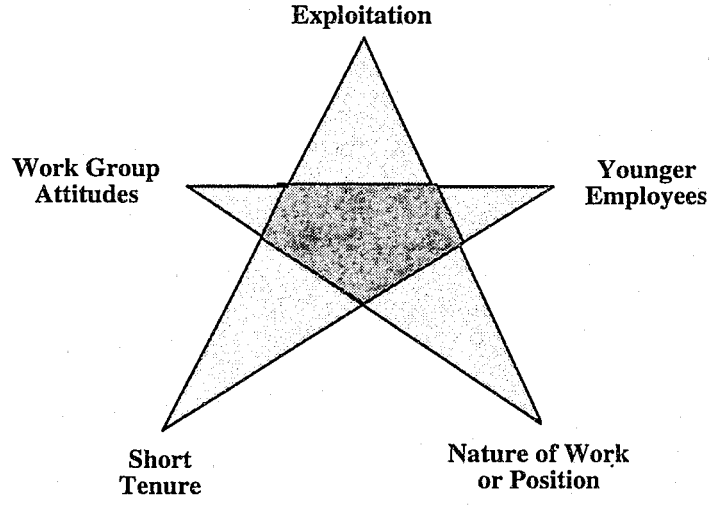
Belief: Most employee thefts involve personal debts. **Fact:** Most employees commonly steal "nickel and dime" amounts unrelated to personal debts. However, gambling debts, love affairs, substance abuse, and/or financial mistakes, can lead to embezzlement or other thefts of large amounts of money.

Belief: Dismissal is the single "best" deterrent to employee theft. **Fact:** Many employees have other job opportunities and/or do not have others depending on their income. Your best deterrent is to create peer-group pressure by carefully explaining policies that employees understand.

THE 5-POINT CONCEPT

The likelihood of employee deviancy increases when there is more than one "trigger" factor present in the work environment; this is exemplified by the "5-point" concept (Figure 4). Take preventive/corrective actions if any of these "points" exist, although they do not confirm that your employees are stealing. You are cautioned not to use them as a crutch: your concern for your general security should remain consistent even if the 5 points are NOT present in your place of business.

FIGURE 4.
FACTORS CONTRIBUTING TO DEVIANT BEHAVIOR



Exploitation and Work Group Attitudes. A negative individual or work group attitude can develop if employees perceive you, or your managers, as exploitative (via poor supervision, support, training, dishonesty, unfairness, indifference, etc.). This creates a *de facto* justification for stealing.

Younger Employees. Employees aged 16 to mid-20s have usually few, if any, dependents or other responsibilities, and thus are often less committed to company goals, less likely to conform, and may not be responsive to the social risk associated with being "caught" and terminated.

Short Tenure. Short-tenured or rapid-turnover employees do not perceive theft as jeopardizing their (nonexistent) seniority rights or long-term employment prospects.

Nature of Work or Position. Some jobs provide more autonomy and freedom, and a greater opportunity for theft. Highly skilled and educated employees—e.g., your accountants or controller(s) in charge of your books, records, and money—are well-placed to "steal you blind."

Your efforts to reduce opportunities to steal will deter those employees who are basically honest. Avoid hiring deviantly-inclined employees, who will not be deterred by your most elaborate security procedures. If you want to trust your employees, hire trustworthy employees.

WHAT CAN I DO ABOUT EMPLOYEE THEFT?

Employee theft is "rule-breaking" behavior within an organization, and thus a management issue. You can manage it as you do other forms of deviance (e.g., absenteeism/lateness) through prevention and employee involvement.

Assess Your Vulnerabilities. Your type of business probably has an "optimal" pattern of dishonest conduct that deviant employees will follow. If cash transactions are a primary function, focus on potential avenues for cash diversions. If you have warehouse or loading-dock employees, examine how and where they could hide or remove merchandise. Ask yourself how employees might invoice below-established prices to receive "kickbacks" from customers; how employees might pilfer merchandise covered by "doctored" inventory lists; or how employees might use company time, facilities, or computers for personal gain. You need to observe your workplace environment, your employees' behavior, and how your products or services are handled to gain a complete picture of your vulnerabilities.

Involve Employees. Regularly "shop-talk" to encourage teamwork, share information, and talk about your business success(es). Your employees will learn that protecting company property and assets from theft and other deviant acts is in their best interest, because their job security is inextricably linked with your business security. The peer-group environment in your business, supported and enforced by your formal policies about security and crime prevention, is key to controlling employee deviance.

John P. Clark and Richard C. Hollinger, *Theft by Employees in Work Organizations: Executive Summary* (National Institute of Justice, Washington, DC), 1983.

Richard C. Hollinger, *Dishonesty in the Workplace: A Manager's Guide to Preventing Employee Theft* (Park Ridge, IL), 1989.

PART II. EMPLOYERS' RESPONSIBILITIES

A. YOUR COMPANY CULTURE

Crime is a Symptom—Poor Management the Disease

Evaluate your corporate environment—and perceptions thereof. How do your employees view you and your business from their perspective? Do they feel manipulated or exploited to increase your corporate profit? Do they see you "gouging" your customers with high prices, or "strangling" your suppliers with slow payments? Do your employees feel ignored, or unworthy of your trust and loyalty?

These questions are important, because your corporate environment cannot be separated from the daily example you set for your managers, supervisors, and employees. Like it or not, you have the ultimate responsibility to establish the standards—integrity versus selfishness, fair dealings versus exploitation—for the business climate from which your employees will take their cues.

Why should you be concerned about your employees' perceptions? A survey by the National Institute of Justice on this subject concluded that:

> "...those employees who felt that their employers were genuinely concerned with the workers' best interests reported the least amount of theft and deviant behavior. When employees felt exploited by the company or their supervisors (those who represent the company in the eyes of the employees), we were not surprised to find employees most involved in correcting this perception of inequity or injustice by acts against the organization."

Your employees are your primary asset; they define your company for customers and competitors alike. You need to work to prevent your employees' "first day" enthusiasm and cooperation from turning into dissatisfaction or deviance.

KEY EMPLOYER RESPONSIBILITIES

- CONDUCT THOROUGH PRE-EMPLOYMENT SCREENING
- MAKE EMPLOYEES PART OF YOUR LOSS PREVENTION PROGRAM
- PREPARE AND DISSEMINATE A CLEAR AND WELL-DEFINED COMPANY POLICY MANUAL
- SCHEDULE REGULAR MEETINGS WITH EMPLOYEE'S OR THEIR REPRESENTATIVES

YOUR POLICY AND PROCEDURE MANUAL: WHY

Your responsibility extends beyond word-of-mouth. Set your standards—your company's values—into formal, written company policies. Your policies should clearly define acceptable and unacceptable behavior and should cover the entire range of conduct potentially detrimental to the welfare of your company. Your policies must cover the sanctions to be levied for violations of your written directives.

Failure to assume the responsibility of formulating and disseminating policy not only is unfair to your employees, but is potentially fatal to your company.

COMPANY POLICY ON DEVIANT BEHAVIOR

CONTENT

- **DEFINES EMPLOYEE CONDUCT DETRIMENTAL TO THE COMPANY**
- **DESCRIBES CONTROL SYSTEMS WHICH DISCOURAGE DEVIANT BEHAVIORS**
- **IDENTIFIES RESULTING DISCIPLINARY ACTIONS**
- **EXPLAINS HOW SANCTIONS WILL BE APPLIED**

Too often your employees will devise their own *de facto* policies that can run counter to the successful operation of the company. These informal procedures are often the result of employees observing that the unsanctioned activities of fellow employees receive little, if any, response from you or their supervisor. If deviance in your company goes undetected or unpunished, it will increase and quickly come to constitute the accepted norm for your employees.

The overwhelming importance of written policies regarding deviance was reported in a study by the National Institute of Justice, which concluded that:

- Companies cannot simply rely on society's general prohibitions against theft.
- Company policies must be "alive" (i.e., regularly updated in response to environmental changes), and "breathing" (i.e., regularly communicated to the work force).
- Established sanctions must be uniformly and consistently imposed; written sanctions without muscle wreak greater harm than does silence on the subject.
- Events requiring sanctions against the responsible employees must be communicated to your general work force, so that others can reasonably calculate their risks and costs of getting caught.

Clearly communicate your written policies to both new and existing employees. This requires little effort at the time you start your business, but much more when you are well established with numerous employees. Avoid training "at random;" instead, train from your documentation of how you want your business to operate. This is your opportunity to delineate your rules and set the tone for your business environment and operations.

COMPANY POLICY ON DEVIANT BEHAVIOR

IMPLEMENTATION PROCEDURES

- **PROMULGATE TO ALL EMPLOYEES**
- **VERIFY THAT EVERY EMPLOYEE UNDERSTANDS POLICY**
- **INCLUDE ORIENTATION ON POLICY WHEN TRAINING NEW EMPLOYEES**
- **CONDUCT PERIODIC RETRAINING ON POLICY AND DISCIPLINARY ACTIONS**
- **ENSURE UNIFORM ENFORCEMENT OF POLICY**

YOUR POLICY AND PROCEDURE MANUAL: WHAT

Clearly understand the issues you need to address when you publish your company manual. Drafting it may seem intimidating, but most of your policies will be straightforward. You may model your own policies on the sample policies provided in Part VI of this *Guide*. Please note you should define policy, provide avenues for investigation, and clearly identify possible sanctions against employees violating policy.

A basic company policy manual can be divided into five major categories that provide adequate coverage for an informed work force. These categories and suggested topics therein include:

Company Mission and Manual Administration

- Letter from the president;
- History of the company;
- Company's mission, philosophy, and goals;
- Manual distribution and adherence to content;
- Additions, updates, and deletions to manual.

Employee Benefits and Working Conditions

- Company amenities (insurance, discounts, pension, parking, etc.);
- Leave policies (vacation, holidays, special leaves, overtime compensation, etc.);
- Promotions;
- Payroll procedures, work hours (including lunch and break periods), smoking policy and areas, attendance and access to company property, telephone use;
- On-the-job injuries;
- Discharge, termination, layoffs, etc.

Employee Behavior

- Sexual harassment, and sex, race, and disability discrimination policies (a model sexual harassment policy appears in this *Guide's* Part VI);
- Drug free work force policy See Part VI;
- Appearance standards;
- Deviant behaviors and disciplinary actions;
- Solicitation on company property.

Asset Loss Prevention - Internal

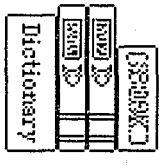
- Crime and loss awareness and prevention policy;
- Money handling policy;
- Company property, equipment, and materials;
- Information and computer protection;
- Inventory policy and procedures;
- Emergency procedures.

Asset Loss Prevention - External

- Robbery and burglary procedures;
- Shoplifting prevention procedures;
- Check and credit card procedures;
- Positive identification procedures.

LEGAL CONSIDERATIONS

The vast body of federal, state and local statutes and regulations controlling employer/employee relations are directed at the rights of employees and the obligations of employers. Some cover actions an employer can take to protect assets from dishonest employees, including: employment selection procedures, surveillances, eavesdropping, searches, investigations, interviews, fingerprinting, drug testing, and use of polygraphs. Some investigative methods may be lawful under certain circumstances, but illegal under others. Some of your policies will therefore require more technical or legal understanding. When in doubt about any policy, consult your attorney.



John P. Clark and Richard C. Hollinger, *Theft by Employees in Work Organizations: Executive Summary* (National Institute of Justice, Washington, DC), 1983.

In General: J. K. Barefoot and D. A. Maxwell, *Corporate Security Administration and Management* (Stoneham, MA), 1987.

William E. Hartsfield, *Investigating Employee Conduct* .

National Crime Prevention Council, *Guide for Corporations to Help Prevent Employee Victimization At Work—At Home—In the Community* (Washington, DC), 1986.

B. DRUG-FREE WORKPLACE

How to Keep Your Business "One Step Ahead"

Drug and alcohol abuse is pandemic in our society: no one is exempt from its effects—our families, neighborhoods, schools, and businesses such as yours. Drugs affect your workplace safety and your employees' productivity. Your responsibility is to create and maintain a drug-free workplace. This means establishing drug and alcohol policies for your company, implementing employee drug awareness programs, and even assisting employees to get help for drug or alcohol problems.

WHY SHOULD I BE CONCERNED ABOUT SUBSTANCE ABUSE?

Recent studies indicate that 10-30% of our work force live a drug-oriented lifestyle and 70% of all illegal drug users are employed. A national study of youth has estimated that 7% of those aged 19-27 use drugs at work. It is very probable that one or more of your employees is involved in some form of substance abuse.

Substance abusers are a not-for-profit element of your business. In additional to destroying their personal health, their habits can endanger themselves and destroy your business. You pay real $$$ for substance abusers' "sick" leave, tardiness, absenteeism, overtime, insurance and workers' compensation claims, damage to equipment, and theft. Two studies estimate business costs attributed to substance abuse at $36.3-$50. billion. Another study reports a $7,261 annual cost per substance abuser. Your other less obvious and generally undocumented losses due to drug abuse are diverted supervisorial/managerial time, friction among workers, poor decisionmaking, and personnel turnover.

Your battle, however, will not be lonely. Of employers recently surveyed:

- 76% recognize drug abuse as a serious problem in the general work force;
- 11% have identified drug abuse as a serious problem in their own business;
- 10% acknowledge some of their employees regularly work under the influence of drugs.

As you can see, to claim *"Not in my business!"* denies reality. Drugs do not always happen to the other person!

Federal, state, and local laws already exist that may require your business to become drug-free. Some of the more significant federal statutes include:

- Drug-Free Workplace Act, 41 U.S.C.A. Sec. 701(a)(1), (Supp. 1991)
- DOT Drug Testing Requirements, 49 C.F.R. Parts 391 and 394
- DOD Regulations, 48 C.F.R. 252.223.7500 (1988)

State laws requiring contractors to have drug-free workplaces are already in effect in California, Georgia, Illinois, Maryland, and South Carolina. Florida even enforces bidding preferences for companies having drug-free workplace policies in place.

YOUR APPROACH TO A DRUG-FREE WORKPLACE

Ideally, you should equitably address prevention, detection, and correction. But you need to first identify your primary focus: **reducing** the supply or the demand. Supply-based strategies stress interrupting drug *flow* at any point prior to the ultimate user. Demand-based strategies stress weakening the user's *desire* through a variety of approaches such as education, deterrence (e.g., job loss, criminal sanctions, etc.), rehabilitation, or drug treatment.

Whichever your focus, *you cannot afford to avoid* adopting a comprehensive workplace drug use policy. A 1990 survey showed that, whereas in 1988 only 9% of employers had a written policy on employee drug use, 14.6% had written policies in 1990; likewise, only 6.5% of com-

panies had Employee Assistance Programs in 1988, versus 11.8% in 1990.

You need not be draconian in your approach to workplace substance abuse, but merely reasonable and responsive to your company's operations (and fully aware that your efforts on this issue will effect operations). You should first identify the purpose(s) of your policy, which are usually (1) to prevent your employees from becoming substance abusers, and (2) to assist them to overcome drug and alcohol problems. Also bear in mind that your program must respect and protect your employees' rights to privacy.

Procedurally, move sequentially through the following steps:

Awareness and Information. You and your managers need to know the nature, extent, and consequences of substance abuse within your current and prospective work force market.

Policy Development, Education, and Training. Disseminate your written substance abuse policy to ALL employees. Train all supervisors and appropriate employee representatives about drugs and drug paraphernalia; the signs and symptoms of substance abuse and its effects both on- and off-the-job; and the legal, physical, and psychological consequences of continued abuse.

Resource Identification and Referrals. Provide all employees with accurate information regarding public and private assistance resources.

STEPS TO IMPLEMENTING A SUBSTANCE ABUSE PROGRAM

- PREPARE COMPREHENSIVE SUBSTANCE ABUSE POLICY
- DISCUSS POLICY WITH LEGAL ADVISOR AND EMPLOYEE UNIONS
- DISSEMINATE POLICY TO ALL EMPLOYEES
- EXPLAIN POLICY TO ALL EMPLOYEES
- OBTAIN SIGNED POLICY AGREEMENT FORM FROM ALL EMPLOYEES
- ENFORCE POLICY UNIFORMLY

YOUR COMPANY POLICY AND PROGRAM

Problem Recognition. You can learn of employee workplace drug use or trafficking in several ways.

- Your supervisors or appropriate security personnel can report observations of employee behavior suggestive of on-the-job drug use. These may either be direct observations, inferences (e.g., an employee's reduction in productivity after lunch break), or a discovery of drugs or paraphernalia on company property.

- Employees can report observations of coworker drug use or trafficking at the workplace.

- Local law enforcement officers can inform you of suspicions of drug trafficking at your workplace.

- You can review newspaper reports of arrests to learn of employees' off-duty drug use or trafficking.

Employer Response. Your response to information about possible substance use or trafficking in your workplace should depend upon the source and strength of your information, but must be based on explicit and written policy guidelines. At minimum, your policy must tell employees what disciplinary responses will result from discovery of drug use or trafficking. A distinction between employee drug use and drug trafficking is a key element of any employer's

drug policy. Adoption of a drug policy can have several positive legal consequences.

- It is required by the federal Drug Free Workplace Act of employers having contracts with the federal government. Failure to adopt or enforce a drug policy can result in loss of federal contracts.
- It helps the employer meet its obligations under health and safety laws for a safe workplace. Such obligations may arise under state law (e.g., workers' compensation, safe workplace laws) and under federal law (Occupational Safety and Health Act).
- It provides the basis for employer disciplinary actions to enforce its policy. This reduces the potential for litigation over the reasonableness of the employer's actions.
- It can act as a deterrent for employees who now have reason to be concerned about enforcement of policy, including actions to detect violations of the drug policy.

A model substance abuse policy appears in this *Guide*'s Part VI. With minor modifications, that policy should fit most of your needs, regardless of your business type or size. It covers the following key factors:

Policy Philosophy. A statement of your company's rationale for establishing this policy, which can simply identify the nature and extent of substance abuse problems in the work force/workplace.

Identification of Unacceptable Behavior. A clear description of the drug- and alcohol-related behaviors which are prohibited, and the sanctions attached to those behaviors.

Methods of Detecting Violations. A listing of your investigative policies, including the circumstances under which investigations will be undertaken (e.g., drug testing, facility searches, etc.), and the consequences for proven violations.

Education, Prevention, and Treatment. An outline of your drug-free awareness program, informing employees about the dangers of substance abuse and the availability of drug counseling, rehabilitation, and Employee Assistance Programs (EAPs).

Rehabilitation Programs. If you are not already required by regulation to have a rehabilitation program, you may wish to consider establishing or "buying into" an Employee Assistance Program. EAPs exist to provide employees having personal problems affecting their work or productivity with assistance via information, advice, counseling, or referral. EAPs handle problems ranging from addictions and neuroses to locating child care. EAPs maintain an employee's dignity and confidentiality, facilitate positive management/labor relations, and encourage a problem-resolution approach to issues affecting your workplace. EAPs thereby provide a real return on your initial investment in both the EAP and your employee.

Your EAP should be open to all employees on a self-referral or a supervisory referral basis. With exceptions only for sensitive positions, no employee's job security or promotional opportunities should be jeopardized by a request for counseling or referral to outside assistance. The EAP's purpose should never be punitive.

Operate your EAP under a clearly defined policy that outlines its purpose, organizational and legal mandates, employee eligibility and applica-

tion procedures, and the roles and responsibilities of involved personnel.

Enforcement Program. Enforcing a substance abuse policy is difficult, but the following "bedrock" will help ensure your effort's success:

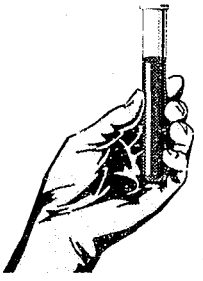
- You and your managers must have a complete understanding that this program will affect your operations.
- Your employees must completely understand your company's performance standards and enforcement procedures.
- You must protect your employees' rights to "privacy" at all times.
- Your enforcement actions must be guided only by your primary goal: to assist employees to overcome substance abuse problems.
- You must deal severely with "for profit" drug trafficking, to include criminal charges.

Drug trafficking/profiteering. Drug distribution and drug use may be related phenomena, but they are not comparable. Drug trafficking depends upon buyers, but drug sellers may not be users, and *vice versa.* Two types of drug trafficking occur in the workplace. The most common is a non-profit employee "sharing." The other involves actual profiteering, rather than trading favors, and requires the trafficker to "market" his goods (i.e., to persuade others to buy). Workplace drug use often increases where drug profiteering exists. You can expect some drug trafficking in any business with 25 or more hourly employees.

You have substantially more discretion in your policies and enforcement measures against drug traffickers than you do against drug users *per se.* The latter are protected by federal laws prohibiting discrimination against the handicapped, which include recovering substance abusers.

Program Assessment. Regularly monitor the effectiveness of your substance abuse policy and program. Regular assessment, including the nature of your business, the extent of workplace drug use, and the costs of your drug program, will allow you to tailor it to meet new or unforeseen circumstances.

To Test or Not to Test?



While few states have comprehensive laws requiring substance abuse testing by private employers, this does not prevent employers from substance abuse testing. A 1991 Department of Labor national survey of private and public employers showed that 11.9% of all drug tests were confirmed positive. That is, more than one in ten of those tested in the work force have drugs in their system. Can your business operate safely, efficiently, and securely, if over 10% of your employees are involved in drugs?

ELEMENTS OF A COMPREHENSIVE SUBSTANCE ABUSE PROGRAM

- Written Substance Abuse Policy
- Supervisory Substance Abuse Identification Training Program
- Employee Substance Abuse Education/Awareness Program
- List of Available Resources for Employees and Supervisors
- Available Employee Assistance Program or Referral
- Drug Testing Program Where Appropriate:
  - * Pre-Employment
  - * For Cause
  - * Random
- Disciplinary Procedure for Violations of Policy

Certain contracts with federal, state, or local governments, or with private institutions, require employers to have an operational drug testing program. For example, if your business involves interstate transportation, the U.S. Department of Transportation requires testing for drivers under the following conditions:

- Pre-employment;
- Periodic medical examinations;
- Reasonable cause;
- Random;
- Post-accident.

If you are a defense contractor, the U.S. Department of Defense contract rules require testing under the following circumstances:

- Reasonable suspicion;
- Post-accident or unsafe action;
- Follow-up to counseling or rehabilitation for substance abuse;
- Voluntary testing program;
- New hires.

Some private corporations with drug testing programs may also require sub-contractors to perform certain types of drug testing for their employees.

Planning a Drug Testing Program

If you include drug testing in your company's policy, its use must be based on carefully developed drug testing protocols. You should plan to use confirmatory tests, strict chains of custody and specimen control, reliable (validated) testing procedures, and organizations that have a proven testing track record. You will also need to identify the type(s) of testing you want for the kinds of drugs you will test for, who will be tested, and the consequences of positive test results. Your employees should review all aspects of your testing program and have a right to a re-test of the original specimen.

While supporting your company's policies and standards of conduct, substance abuse testing may also reduce your liability for accidents or other on-the-job problems. Ask your attorney/legal advisor to review your drug testing program for compliance with applicable statutes, regulations or agreements mandated or in effect (e.g., disability discrimination provisions, collective bargaining agreements, etc.).

Designing and Implementing a Drug Testing Program

The design of your drug testing program should be as carefully planned as any other new, critical project: it should be legally sound, well documented and understood by your employees, impartially operated and enforced, and should provide adequate employee safeguards. Your goal—to protect your business (versus to threaten your employees)—will gain credence if you appoint an employee representative to your planning committee.

- **Disseminate and publicize** your written substance abuse policy prior to initiating a testing program. The policy should state when testing will occur: pre-employment (do not forget re-hiring in cases of layoffs), for cause (specify the types of causes), random, enrolled in treatment, etc. It should also specify what will happen if the test is positive.

- **Give proper notice**, via thorough and appropriate employee education/training, that you will implement a drug testing program. After the training sessions, retain attendance records, and obtain signed statements that the attendees understood the specified course content.

- **Ensure all tests are conducted by certified laboratories**. The National Institute on Drug Abuse (NIDA) certifies drug testing laboratories and requires adherence to uniform standards for "confirmed positives" on selected substances. Contact your state department of health and mental hygiene to obtain a list of certified labs in your state, and any specific state regulations; for example, Maryland requires that any laboratory used for drug testing must be certified by the Maryland Department of Health and Mental Hygiene (Human Services).

- **Arrange a formal review of all test results.** You can contract with, or create, some form of Medical Review Office (MRO) for this purpose. An MRO makes medical judgments on "false positives" caused by prescribed drugs or food. It also ensures your program's credibility by regularly reviewing the program's adherence to policy and procedures regarding: confidentiality; prevention of dilution, alteration or substitution; chain of custody; and appropriate treatment, referral, or disciplinary actions. Some form of regular monitoring of your entire substance abuse policy and program is essential.

WHAT A CERTIFIED LABORATORY SHOULD PROVIDE

- STRICT CONFIDENTIALITY
- GUIDANCE IN ESTABLISHING ON-SITE SCREENING PROCEDURES
- LOCATION(S) FOR OBTAINING SAMPLES
- PREVENTION OF DILUTION, ALTERATION, OR SUBSTITUTION
- STRICT CHAIN OF CUSTODY
- EXPERT WITNESS DURING LITIGATION OR ARBITRATION

William F. Banta and Forest Tennant, *Combating Substance Abuse in the Workplace*, 1989.

Bureau of Business Practices, *Drugs in the Workplace: Solutions for Business and Industry* (Waterford, CT), 1987.

Governor William Donald Schaefer, *Maryland's Drug-Free Workplace Initiative: Keeping Maryland Business a Step Ahead* (Annapolis, MD), 1992.

Institute for a Drug-Free Workplace, *A Guide to State Drug Testing Laws and Legislation* (Washington, DC), 1992.

National Institute on Drug Abuse, *Model Plan for a Comprehensive Drug-Free Workplace Program* (Rockville, MD), 1989.

PART III. SIGNIFICANT SECURITY ISSUES

A. EMPLOYEE ISSUES

Protect Your Most Important Asset

The need to create the proper atmosphere with your employees starts, quite aptly, at the beginning. Put simply, if you don't hire problem employees, you will have a much better chance of preventing future problems. In many ways, this is the most critical area to initiate the process of preventing theft, substance abuse, and other deviant behavior in your work force.

The second step is to provide these "screened" employees with your corporate vision and specific guidelines on how you want the company to operate. The new employee must know what is expected and how to function within the corporate culture. Each employee should receive a copy and instruction on the company's policies and procedures.

Once you have the screened employee in place, you must begin to indoctrinate the employee with loss awareness and prevention techniques. If possible, new employees should be oriented not only to the policies of the company, but also to the importance of keeping the company financially healthy and the part each employee plays in reaching that goal.

As part of this asset protection effort, the company should create a method by which concerned employees can report conduct injurious to the company. This can be done through hotlines, or any other method of communication that allows for anonymity and timely response.

1. PRE-EMPLOYMENT SCREENING: *Success Depends on Hiring the Right People*

BEFORE YOU INTERVIEW: WHAT SHOULD YOU DO?

All companies "live or die" on their ability to recruit, screen, hire, and train quality employees, but few screen well—if they screen at all. Do not interview only for potential performance on the job; you must go beyond past performance and experience.

TOOLS USED TO SCREEN POTENTIAL EMPLOYEES

- INTERVIEW PROCESS
- PRE-EMPLOYMENT BACKGROUND CHECK(S)
- JOB-RELATED PERFORMANCE TEST(S)
- PSYCHOLOGICAL SCREENING(S)
- APTITUDE TEST(S)
- CERTIFIED PREDICTABILITY (HONESTY) INDEX TEST(S)

Professional recruiters advise you to:

Start With a Clear, Written Position Description. Using your employee records, identify the characteristics that made any predecessors successful, and whether prior work experience was an important factor. Your written position description should include all necessary characteristics and prior work experience, and should exclude any characteristics or causes of prior failures.

Standard elements of your job description should include:

- Educational requirements. What education will translate directly into job success? Also, consider the education applicants may need for their *next* position in your company—you need to hire promotable people.
- Previous experience. Do not limit your search to persons who have merely done the same job for a competitor. Instead, consider what "crossover" skills might suit your position, (e.g., a former bookkeeper might be appropriate for legal research because each job requires attention to detail). Such employees will be more valuable to you in terms of versatility and development.
- Compensation. Always recruit based on a fair compensation package for your particular labor market. Inadequate compensation can be demoralizing, increase turnover, and may lead disaffected employees to rationalize internal theft (i.e., to augment your below-market compensation).
- Job duties. Specifically list all duties and responsibilities for your new employee, to avoid myriad problems arising from misunderstood and/or unrealistic expectations. You must also incorporate and communicate other hiring requirements in your recruitment (e.g., the *Americans with Disabilities Act* requires you to provide "reasonable accommodations" for disabled employees, who may need equipment or facility modifications, or even job restructuring).
- Intangibles. Do you require other characteristics—stability, energy, temperament, etc.—in your ideal candidate? If so, specify them in your position description and follow-up in your interview questions.

Review your completed position description to see if your requirements—education, experience, compensation, etc.—are compatible with your list of job duties. Adjust your requirements or job duties if needed.

Require All Candidates to Complete a Job Application Form. If you ignore the application, you will never "see" your candidate's advantages (or liabilities) in abilities and personality. A comprehensive application form should contain:

- Personal information: the applicant's full name, residential address, phone number(s), social security number, and driver's license number;
- Specific details about employment history, educational background, and personal references; and
- A signed waiver allowing you to conduct a complete background check (refusal to sign should signal you to terminate that applicant's recruitment).

EMPLOYEE APPLICATION FORM
REQUESTED INFORMATION

1. **IDENTIFICATION**
   - Name(s), address(es), telephone number(s), and social security number.
2. **POSITION DESIRED**
3. **PREVIOUS EMPLOYMENT**
   - Names, addresses, telephone numbers, positions, and salaries.
     * *"Have you worked for us before?"*
     * *"Can we contact your previous employers?"*
4. **EDUCATION AND TRAINING**
   - Names, locations, and dates of high school, college, and other training or technical certifications, work permits, licenses, etc.
     * *"Can we contact your school(s) for transcripts?"*
     * *"Do you have legal authorization to work in the U.S.?"*
5. **PERSONAL REFERENCES**
6. **MILITARY SERVICE**
   - Dates, branch of service, and training received.
7. **CONVICTIONS**
   - Dates, jurisdictions, and crimes
     * *"Have you been convicted of a felony in the last five years?"*
8. **WAIVER OF BACKGROUND CHECK**
9. **SIGNATURE OF APPLICANT**

EMPLOYEE APPLICATION FORM
REQUIRED INFORMATION

1. **STATEMENT THAT COMPANY HIRES ON QUALIFICATIONS *ONLY*—regardless of race, color, sex, national origin, age, or disability.**

2. **STATEMENT EXPLAINING *ANY* PROBATIONARY EMPLOYMENT PERIOD, CONTINGENCIES (e.g., a satisfactory reference/background check), OR REQUIRED TESTING(S) (e.g., skills, drugs).**

3. **ANY REQUIRED STATEMENT OF STATE OR LOCAL *PROHIBITIONS,* (e.g., Maryland: "State statute essentially prohibits the use of polygraph testing for the purposes of employment or continued employment").**

4. **STATEMENT THAT EMPLOYEES ARE SUBJECT TO *DISMISSAL* IF THEY ARE PROVEN TO HAVE VIOLATED LAWS (e.g., theft, drugs, battery) WHILE WORKING OR ON THE PREMISES.**

Keep all applications; use them to justify hiring (or declining) an applicant or to help you identify those skills you have "on tap" for use or development.

Prepare Your Interview Questions. Your time spent preparing interview questions will ensure that you ask only necessary questions, and that you ask everyone the same set of questions. You

cannot ask about age, marital status, or sexual preference. Additionally:

- You cannot ask about an arrest record (you can ask about **convictions**);
- You cannot ask about a woman's child-care responsibilities (i.e., you cannot assume that only females are responsible for child-care);
- You cannot ask about disabilities or medical history (including prior drug or substance abuse history), according to the *Americans with Disabilities Act* .

Other federal, state, and local statutes and regulations concerning the hiring process may apply to your business; contact your legal advisor regarding specific questions you may wish to ask prospective employees.

Your Interview

With the job description and completed, signed application form before you, use the following techniques during the interview:

Put the Applicant at Ease. Encourage relaxed, candid conversational responses.

Verify Applicant Data. Carefully inquire about information provided on the application; ask about gaps in employment history or incomplete answers. Remember, applicants unable to follow directions on the application may be unable to follow directions on the job.

Take Notes. It is too easy to "misremember" individual credentials after you have interviewed several people. While taking notes as the applicant answers questions, refer also to the job description so you can evaluate the candidate's previous experience and/or training in view of your company's needs.

Listen to Your Instincts. Ask specific questions to clear up any concerns. At this point, your "intuition" is a valid, important part of the process.

KEY ELEMENTS OF AN EMPLOYEE SELECTION PROCESS

- Require All Applicants to Complete an Application Form
- Conduct Thorough Interviews, Verifying Application Information
- Clarify Employment Gaps or Incomplete Responses
- Have Applicants Sign Waivers on Background Checks
- Contact All Previous Employers, Personal References, and Schools
- Keep Completed Application Forms and Background Check Materials

After You Interview

Your background check is the most essential—but difficult and time-consuming—part of your recruitment. Do not rush to fill your vacancy with your "impressive" applicant. A recent *Wall Street Journal* article reports that 30% of applicants significantly misrepresent themselves.

You should also know the incidence of violence in the workplace has risen dramatically in recent years. It is often directed against managers, supervisors, and the owners of small- and medium-sized businesses. In many cases, this violence is perpetrated by disgruntled employees with past histories of violence and deviant behavior. Invariably, many of these individuals would not have had the opportunity to victimize you, or your employees, had you known more about their past criminal convictions, substance abuse history, or related problems. Your background check can be a proactive measure to ensure your and your employees' safety.

Protect yourself: do the following basics:

Verify the Application's Data. Any misrepresentation discovered now probably constitutes

both a lie on the application form and a lie in the interview. If applicants cannot safeguard their own integrity, they will not safeguard your assets.

- Call previous employers. Ask if they would hire this person again. Even "close-mouthed" companies will usually admit whether or not a candidate is "eligible for rehire." Look for an unhesitating, affirmative answer; reluctant or roundabout replies should signal suspicion on your part.
- Contact personal references. Ask them not only about the applicant's positive traits but also about work history. Many are very candid about why someone left a former job, and will detail (briefly or at length) the contributing "cause(s)" that can affect your decision-making.
- Check other sources. Do not assign company vehicles to new employees with histories of driving violations, or hire cashiers with histories of financial troubles. While you cannot ask about age *per se*, once the employee is hired, you may request date of birth to allow you to conduct and cross-check a criminal conviction record investigation. Certain records—credit, driving, worker's compensation claims, and any criminal convictions should be readily available to you. You can use a criminal conviction record to examine your candidate's application and interview candor. (The Equal Employment Opportunity Commission, however, has ruled that you cannot deny employment solely because of a criminal record, if the nature of the crime is not relevant to the job.)

You may want to hire an investigative agency if you need to know a lot about an applicant's background. The *Fair Credit Act*, however, dictates that you must notify an applicant when you seek an outside agency's investigative services, but only when you use its report in connection with an employment decision.

Use Pencil-and-Paper Honesty Tests.

Candidates can be asked to take appropriate tests (e.g., job-related employment, aptitude, or psychological tests), but only after they have successfully passed your background screening. These tests should have substantially less impact on your screening process than your background check, if only because some tests have recently been called into question due to the possibility of their manipulation (consult your legal advisor or personnel expert in this regard).

Wall Street Journal, "Job Interviews Pose Rising Risk to Employers," March 11, 1992.

In General: National Employment Screening Services, *The Guide to Background Investigations* (Tulsa, OK), 1990.

Art Buckwalter, *Interviews and Interrogations* (Woburn, MA), 1981.

B. E. Gorill, *Effective Personnel Security Procedures* (Homewood, IL), 1974.

Dale Yoder and Herbert Heneman, eds., ASPA *Handbook of Personnel and Industrial Relations* (Washington, DC), 1979.

2. CRIME PREVENTION AND LOSS AWARENESS: STARTING SOMETHING POSITIVE.

The challenge to the nation is to make a reality of the idea of prevention, to move beyond intervention. Preventing crime means not just stopping something negative, but starting something positive."

Crime Prevention in America,
Foundation for Action,
"Crime Prevention Coalition"

You must make your employees aware of the impact of internal theft. However, you may be uncertain about what you should share with them. Would they understand—and appreciate—the concepts of net profit, gross profit, and the impact of lost assets (such as an internal theft of $50,000, when your net profit is only 4%)?

Unless you explain, employees will not understand the meaning of any of these concepts. When they learn that rampant theft, poor productivity, and other abuses could result in their potential lay-off or the company's shut-down, motivation and job performance could significantly improve.

INFORMED EMPLOYEES

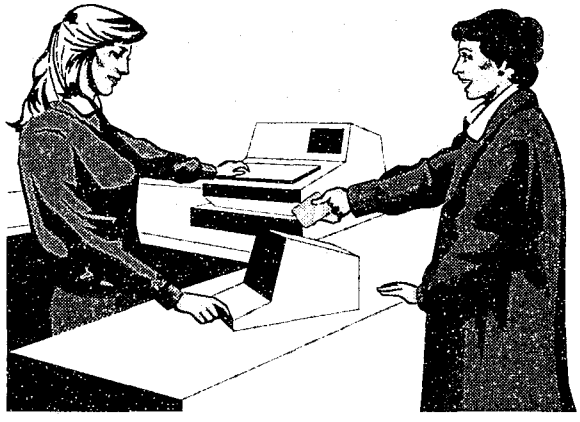
Your employee crime prevention and awareness programs should be an integral part of your business security effort. They not only reduce internal theft and your vulnerability to crime, but can also increase employees' morale, well-being, and productivity.

Before undertaking any such programs, however, you must have your company security policies and procedures in place. Depending largely on the nature and size of your business, you can then determine how to present your security procedures and crime prevention awareness—such as inventory control, cash handling, visitor screening, etc.—to your current, and future, employees. It is best to present them as part of your new employees' basic training, which should be included in all employee manuals or handbooks. A small business can train individually, while larger or decentralized operations should train groups of new employees.

After your initial training, monitor and reinforce procedures to tell employees they are your vital, integral link in the team approach to security and crime prevention. Utilize on-the-job or refresher training, or regular meetings with your employees, so you can solicit and act upon their ideas about loss prevention, stressing that all suggestions for improvements are welcome. Changes to your procedures should be formally added to your existing policies as addenda, not as inter-office memoranda.

ALERT AND CONSCIENTIOUS EMPLOYEES

Your attentive sales clerks—trained to be helpful and aware of shoplifters' techniques—can reduce shoplifting incidents by simply saying, *"May I help you?"* or *"I'll be right with you!"* as a warning of watchfulness. Similarly, cashiers familiar with store prices can help curb "price switch" games.



Fraudulent Identification. It can be painful for smaller companies, particularly where cash flow is critical, when fraudulent or stolen checks or credit cards are accepted—particularly if preventive policies are loose or absent. You could decline all checks and credit cards, to eliminate such problems; however, to be "user-friendly," you need to make your customers' purchasing as convenient as possible while also maintaining

the security of your sales volume. Your policies regarding checks, credit cards, and identifications should be well-formulated, and well-understood by your employees. It should uniformly apply to all purchases, even if the customer is well known to your establishment. Training your employees about your transaction policies will save you from fraudulent purchases.

Because fake IDs are becoming more common, you need to identify the types and kinds of identifications your employees may accept. While all forms of identification can be copied, certain IDs are safer than others. It is harder to create fake IDs when the card has a laminated and recognizable photograph. Many jurisdictions now produce driver's licenses and other official forms of ID which are very difficult to alter, because their backgrounds (through default precautions) foil most attempts to change personal data. Does the check's address match the driver's license address? Does the individual's driver's license match the given birthdate, and apparent hair color, race, sex, and other identifiers on the license? Does the sales slip signature match that on the credit card reverse? **NEVER fail to question these identifiers if they appear to be incorrect on the ID.**

You must be diligent in reviewing the IDs you require from your customers, because your example speaks most loudly to your employees. If you do not scrutinize, your employees will merely follow your example.

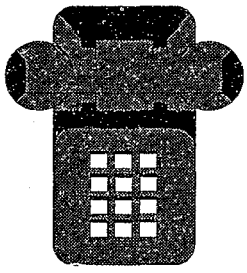
EMPLOYEES' PERSONAL SECURITY

Employers appearing impersonal or indifferent to their employees create an environment conducive to deviant behavior. Remember, all employees are important to your business. Therefore, you would be wise to include materials and information on your employees' personal security in your crime prevention/awareness program.

Examine your work location(s) to identify areas where safety may be compromised (dark parking lots, blind reception areas, etc.), and suggest personal safety precautions about employee workplace behavior and actions. Your business security program can also address employees' at-home and off-work activities. Learn about the victim services in your employees' home areas, so that you can communicate your concern for their welfare. All such information-sharing can be included as part of your company's informal lunch hour program, or—particularly around holidays, winter months, etc.—in memos, bulletin boards, group training, in-house newsletters, or check stubs. Your local law enforcement agency or crime prevention association can assist you with each aspect of your business/employee security program.

3. EMPLOYEE/EMPLOYER COMMUNICATIONS—HOTLINES: *Easy, Quick, and Vital*

CRIME STOPPER HOTLINES



Ours is the age of "hotlines," now in use for all types of communications between product manufacturers and consumers; service providers and customers; and community residents and their police department.

Hotlines cut through "red tape," because people can communicate quickly, simply, and anonymously. The police pioneered hotlines in 1976 when the first community-based Crime Stoppers hotline was formed in Albuquerque, New Mexico, to allow residents to confidentially report crimes or tips about criminal activities. This "self-help" service mushroomed by 1988 to over 600 Crime Stoppers communities. Its success is due to citizens' willingness to provide needed crime information to the appropriate authorities empowered to respond.

BUSINESS HOTLINES

In the 1980s, businesses increasingly adopted employee hotlines because they significantly improved communications between management and employees—communications involving serious matters crucial to the company's well-being which might not occur were a hotline not in place. Your employees could inform you about:

- Thefts of company cash, supplies, materials, or equipment by co-workers;
- The storage, sale, or distribution of drugs on company property;
- Company vehicles or machinery being operated under the influence of drugs or alcohol;
- Embezzlement or fraud involving company assets;
- Abuse of time, leave, or other corporate privileges;
- Diversion of corporate opportunities;
- Sexual harassment.

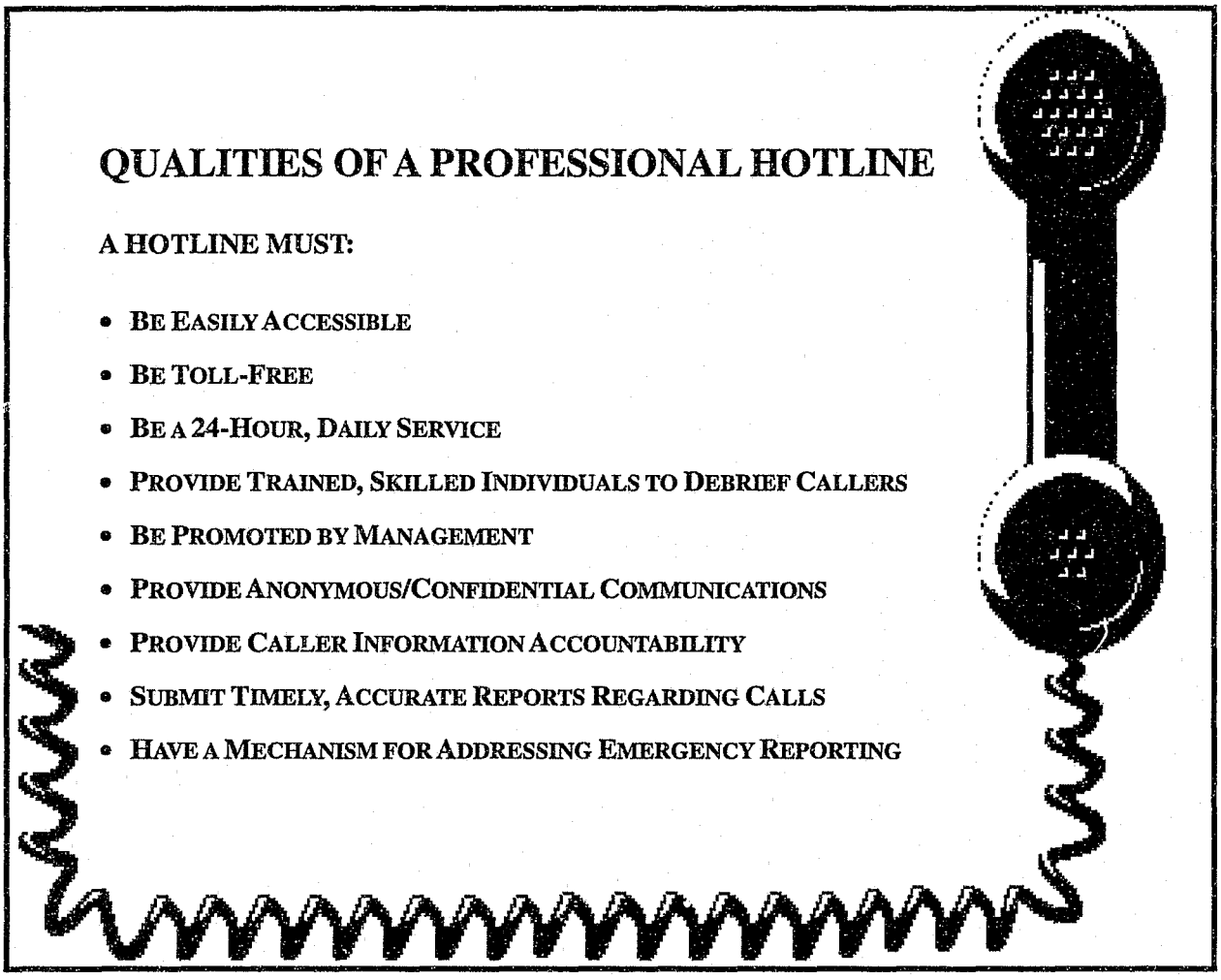
Your ignorance of such critical issues can ruin your business. Only a hotline promising strict confidentiality—even outright anonymity—can bring you this vital information.

HOW TO ESTABLISH A HOTLINE

Your company's size and structure will dictate the nature of your hotline installation. In-house hotlines, normally connected to the human resources department or security office, encourage employees to relay tips or suspicions of workplace loss or deviant behavior to a company official, usually empowered to investigate the matter. A contractual third-party hotline service, on the other hand, uses professional communication specialists who "debrief" callers to obtain essential information. A written report, with a control number for tracking purposes, is then submitted to the client's designated authority. Any further investigation may be undertaken by the client or by another service provider.

Another type of hotline involving the general public, not just your employees or customers, is your company's vehicle bumper stickers (or other signage) with a telephone number that citizens can call to report reckless or discourteous operation.

Make your hotline uncomplicated and advertise its goals in priority order: loss prevention; loss detection; and mitigation of workplace liability. Your professional hotline service—for your employees, customers, and/or the general public—will demonstrate your proactive interest in soliciting information about potential loss issues so you can make immediate corrective responses.


QUALITIES OF A PROFESSIONAL HOTLINE
A HOTLINE MUST:
• BE EASILY ACCESSIBLE
• BE TOLL-FREE
• BE A 24-HOUR, DAILY SERVICE
• PROVIDE TRAINED, SKILLED INDIVIDUALS TO DEBRIEF CALLERS
• BE PROMOTED BY MANAGEMENT
• PROVIDE ANONYMOUS/CONFIDENTIAL COMMUNICATIONS
• PROVIDE CALLER INFORMATION ACCOUNTABILITY
• SUBMIT TIMELY, ACCURATE REPORTS REGARDING CALLS
• HAVE A MECHANISM FOR ADDRESSING EMERGENCY REPORTING

B. INVENTORY AND MONEY CONTROL

1. INVENTORY CONTROLS: *Don't Just Watch Your Assets Walk Out!*

CAUSES AND CONTROLS

Your inventory, often your major capital investment, can be up to 50% of your total capital investment—up to 75% when you include carrying costs, e.g., storage, insurance, taxes, transportation, handling and distribution, depreciation, obsolescence, etc. In 1981, American businesses lost over $5 billion through employee theft, and over $4 billion through outsider's theft. Ten years later, those figures have more than doubled, in part because fewer than 50% of small businesses undertake consistent perpetual or periodic inventories. However, you can deter such losses via an efficient, documented inventory control system.

Although you must have sufficient inventory on hand to fill your orders, which can be complicated for seasonal businesses, a "tight" inventory will help you avoid losses due to obsolescence. If you also increase your inventory turnover, fewer goods (and attached capital investment) will be vulnerable to internal theft. By itself, your greater attention to higher inventory turnover will reduce opportunities for theft and send a clear message about your desire for control.

Maintain a continuous, accurate written inventory control system. Ideally, the system should be streamlined for ease in recordkeeping and "lean" for flexibility and maximum deterrence.

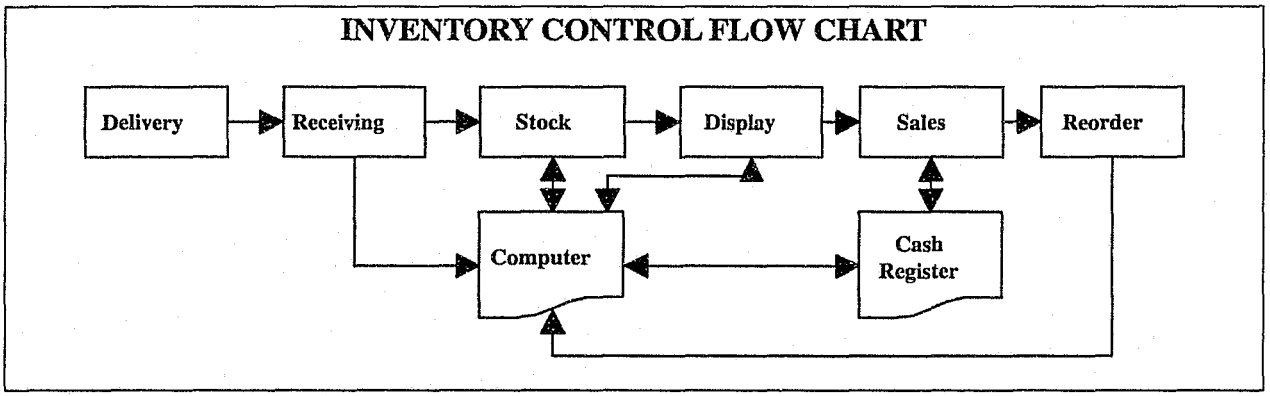
CRITICAL AREAS OF VULNERABILITY

- RECEIVING
- INVENTORY AND STORAGE
- DISPLAY
- SALES
- CASH TRANSFERS
- MAILROOM/DISTRIBUTION
- TRASH DISPOSAL
- OFFICE SUPPLIES/PETTY CASH
- CUSTOMER SERVICES

SETTING UP AN INVENTORY CONTROL SYSTEM

Inventory Data Cards/Ledgers. Master ledgers, preferably computerized, should be maintained in your accounting/production departments (or in your main office) and under the control of someone other than the person who maintains the on-site inventory data cards. Each storage item should have a written or computerized inventory control "card" describing the item, maximum/minimum stock quantity, ordering/reordering quantities, last order date, quantity on-hand/on-order, quantity received/used/sold, and balance-on-hand. The card/ledger system means you can conduct annual (preferably quarterly) inventory audits for quick stock availability checks.

Maintain production/operational cards at your storage areas for raw materials, parts components, supplies, and semi-finished and finished products.



Inventory Control Flow. A computerized inventory management program can provide detailed information about your inventory status, cost analysis, lists for inventory verification, period and year-to-date usage, future inventory projections (and any other data you need for system analysis). It gives you control over all merchandise, stock, and capital equipment. A cyclical software inventory review, available for different businesses, can track stock and capital equipment as it flows through your business cycle (see Inventory Control Flow Chart).

Inventory Control Tips

Capital Equipment

- Attach a numbered tag to identify all capital equipment;
- Audit quarterly and annually;
- Purchase only what you need;
- Use one computer/inventory data "card" for each location listed.

Receiving/Storage Area

- Keep inventory low, short of out-of-stock status;
- Store inventory in well-lighted, visible areas, to discourage pilferage;
- Store items in predetermined, easily countable numbers (e.g., groups of ten on shelves or in bins), preferably in pre-outlined areas;
- Require two employees to receive deliveries, check the manifest against items received, and move the items to storage as soon as possible; police the loading and receiving areas, and beware of "phantom" shipments (to non-customers);
- Keep your shipping and receiving areas securely locked and out-of-bounds to unauthorized personnel; forbid exiting through your inventory areas or stockrooms;
- Use only sealed cartons; prohibit private vehicles at loading dock areas; forbid trash cans, etc., in the vicinity of your inventory areas or stockrooms.

Employee Pilferage/Outsider Shoplifting

If your supplies or merchandise are of the kind, size, or value that might tempt your employees to steal, be aware of the following specific warning signs:

- Personal belongings kept in inventory or storage areas;
- An employee's car parked out of its usual slot, or unusually close to a loading dock or exit point;
- Trash bins placed unusually;
- Irregular visits to controlled areas;
- Early or late check-ins or check-outs.

Ensure that all employees are aware of your commitment to inventory security and the prosecution of pilferers and shoplifters—employees and customers alike. Be aware and cautious of customers who:

- Wear long coats or voluminous clothing;
- Hold elbows tight to the sides and/or walk stiffly (to conceal stolen items);
- Know where to go, or loiter in a certain area but refuse assistance or do not buy anything;
- Carry large shopping bags.

In general, you should also:

- Place mirrors overhead or behind counters;
- Post prominent signs about prosecution of persons caught pilfering or shoplifting;
- Keep small, expensive items under lock and key, whether on display or in storage;
- Control entrance/exit access to your location(s).

Mailroom/Distribution Controls

Control and monitor the handling and movement of all forms of mail (U.S., UPS, Federal Express, interoffice correspondence, etc.) by establishing periodically audited procedures.

- Process and deliver items and packages ASAP;
- Strictly secure and limit access to mailroom areas outside of business hours;
- Closely monitor mailing materials and resources (stamps, postage machines, etc.) during working hours;
- Periodically review mailroom/distribution staff procedures regarding product shipping/receiving, movement of valuable items, and tracing lost or missing items;
- Periodically assess your mailroom's physical condition, as unorganized mailrooms invite loss and damage. Periodically check on employee morale, as unmotivated employees may not safeguard your mailroom's operations.

Trash Disposal

Trash security is important for health, safety, and economic reasons. Unremoved trash can be used by dishonest employees to move stolen items for later pickup or for delivery to another receiver.

- Require at least two employees to check outgoing trash;
- Periodically assess your trash for cash recycling purposes;
- Shred proprietary information before discarding.

Office Supplies/ Petty Cash

Inventory your office supplies (furniture, office machines, computer hard- and software) and other bulk purchases—paper, paper clips, pencils, etc.—at least annually to identify lost, missing, damaged, or stolen items.

- Permanently affix or etch an identifying inventory or serial number on all major equipment items;
- Devise a "paper trail" for all office supplies and equipment. Your record of all sales, losses, damages, and thefts will also prevent duplicative purchases;
- Conduct a quarterly inventory of all high value items.

Your petty cash control can also "make" you or "break" you:

- Designate one "petty cash custodian" to maintain paper records of all disbursements and transactions;
- Keep petty cash in a locked box, placed in a locking drawer when not in use;
- Require a manager to countersign all disbursements over $50; bank excess cash when petty cash reaches its predetermined limit;
- Conduct unannounced, periodic petty cash inspections.

Customer Service

Your customer service department can enhance your business image, increase your profits, and help broaden your asset protection program. To properly handle merchandise returns, shipment losses, duplicate orders, "short" shipments, damaged or refused inventory, and credit, C.O.D., or theft problems, you should:

- Train your customer service employees to appropriately handle customer issues;
- Install appropriate record controls for your debit/credit transactions involving returned/damaged/replaced items, to update and identify your inventory needs.

2. MONETARY CONTROLS: *Your Money is Their Target*

CAUSES AND CONTROLS

Three factors are present in virtually all instances of employee theft: motive, opportunity, and rationalization. Properly designed and consistently applied internal controls not only track the normal incidence of errors or omissions in transactions and recordkeeping but also greatly reduce an employee's opportunity or rationale for theft. For a well-run business, you must foster an environment that supports and reinforces honesty and integrity, by providing effective avenues for employee communication and participation.

Although careless or inadequate internal controls invite undesirable employee behavior, your scale of control should fit your size and type of business. Overcontrol will cost money, reduce productivity and creativity, and create a paper monster which itself will induce more error.

Monetary control involves three basic responsibilities: authorization of transactions; physical custody of assets; and timely recordkeeping. Always divide monetary control among your employees to allow for accountability and security.

CRITICAL AREAS OF VULNERABILITY

- EXCESSIVE AMOUNTS OF CASH ON PREMISES
- INADEQUATE STORAGE AND/OR SECURITY PROVISIONS
- SINGULAR RESPONSIBILITY FOR DEPOSITS
- SCHEDULED DEPOSITS
- UNINVENTORIED PETTY CASH

CASH

Cash is the preeminent target for potentially dishonest employees, because paper money and coinage are physically small, easily disposable, and have inherent value.

- Do not allow large amounts of cash to accumulate in cash registers;
- Withdraw cash frequently from your cash register and place it in your on-site safe;

Do not accumulate too much cash in your safe. As cash builds up, make frequent and discreet bank deposits, preferably during the day and on a variable schedule and route.

ARMORED CAR SERVICES

If you handle large amounts of cash, consider an armored car service, which will usually insure your cash deposits from the moment of pick-up until delivery. These services provide bonded professionals with special security training to evade or deal with would-be criminals. An armored car service can also help you maintain better audit controls over your daily cash receipts, because a chain of signed receipts traces each transaction.

Dual-keyed drop safes give added anti-theft protection because receipts, once deposited, cannot be removed until the safe is opened in the presence of the armored car guard. Some armored car services provide customized services including full money-room services and secure overnight (or longer) storage.

CASH REGISTERS

Your register detail tape is invaluable in controlling employee cash theft. Install the following cash register controls:

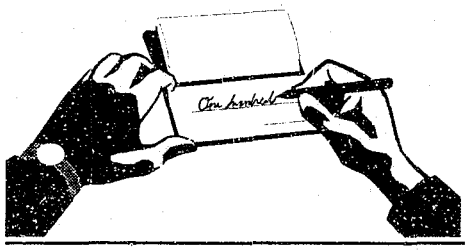
- Ensure that tape transaction numbers are continuous—day-to-day—and match customer receipts;

- Be alert to frequent "over-rings," voids, shortages or overages, and "no sale" transactions. These are also signs of poor or sloppy employees, who are costing you money;
- Assign only one cashier at a time to each register; require them to ring up each sale separately, and fully close the drawer after each transaction;
- Assign a manager to approve all voids, "over-rings," and employee purchases;
- Give customers sale receipts, and run cash register tapes with receipt and detail tapes;
- Empty cash register drawers at closing, and leave them open until your next opening;
- Avoid early or late cashier check-outs: they may be "fixing" the registers to evade your "clean" transaction procedures.

Checks and Credit Cards

Establish written policies and guidelines for cashiers and other employees who accept customer payments by checks and credit cards. Your policy should firmly commit to prosecution and collection of bad checks or credit cards, and could also extend to maintaining a list of persons who have made "bad faith" payments to your business.

Checks



- Require identification, which could include driver's license, credit card(s), and/or military or government identifications;
- Require customers to sign checks in front of the cashier, who should verify the signature against that on the identification;
- Require cashiers to accept checks only to the limit of the purchase, and forbid acceptance of out-of-state checks, which are more difficult to prosecute and collect.

Credit Cards

- Forbid acceptance of expired, altered, or "hot list" credit cards;
- Require matching signatures on both receipt and credit card, and clear all credit card purchases through an automatic approval system;
- Shred or otherwise destroy carbons and voided transaction forms.

"Shopping Services"

No matter how small your business, you could benefit from a shopping service whose business is to detect dishonest employees. Being busy or absent, you may not not the first warning signs of internal theft until your profits start to drop. Seek shopping services through recommendations from fellow businessmen or your business association, or by checking Yellow Page listings under "Security Services." One or two "customers" will be sent to your business to test one (or all) of your employees for signs of on-the-job dishonesty. Some services will also test for courtesy and efficiency, which also affect your bottom-line profit. The fee will vary according to the regularity and type(s) of investigation you require. Properly used, a shopping service can be quite effective, so long as your other controls have "told" you that you need this kind of professional assistance.

C. PHYSICAL SECURITY

Harden Your Resolve—and Your Premises

TARGET-HARDENING

Because your business is vulnerable to both "insider" and "outsider" crime, you need to "target-harden" (protect) your investment, as well as your employees and customers. Do not allow your premises to become an inviting target to amateur and professional criminals because you have not "target-hardened," as your neighboring businesses may have. "Target-hardening" will also alert your employees and customers that you are aware, concerned, and prepared.

Your investment now in effective security protection—crime prevention—means you will not be paying crime costs later. Your options to protect your livelihood range from relatively simple alarms to total electronic protection systems. Do *not* become confused or dismayed by technical sophistication. Do *not* invest in a state-of-the-art system without objectively and rationally assessing your security investment capabilities against your perceived and/or actual risks.

AWARENESS AND CONCERN

When you value your employees' and clientele's well-being by taking steps to protect them, both groups will feel safer and will cooperate with your efforts. Employees will feel more secure knowing that you are protecting your business by protecting their personal security. Customers will also appreciate your attention to their safety, as well as the lower prices you can offer because you are not paying for crime losses.

PREPARATION (PREVENTION/DETERRENCE)

You have a variety of security options (including types and costs) regarding business and personnel/personal protection plans. Because your local police crime prevention unit firmly supports business crime prevention, they will help you "target-harden" so that their resources can be freed for other public safety purposes.

DISABLED CUSTOMERS/EMPLOYEES

You need to review your accessibility by disabled customers and employees (the able-bodied usually ignore the numerous obstacles to business premises) as part of your security plan.

- Are your paths/aisles unimpeded and wide enough to allow wheelchairs, walkers, etc.?
- Do your parking/business accesses provide for the handicapped, including ramps?
- Are your elevator buttons, door handles, drinking fountains, and telephones "reachable" by someone in a wheelchair?
- Do your restrooms have accessible sinks, towel dispensers, toilets, and hot-air hand driers?

1. PROFESSIONAL CONSULTANTS AND VENDORS: *Don't Forget the Experts*

SOURCES OF OUTSIDE ASSISTANCE

Seek advice about internal security issues and prevention strategies from alarm company representatives, locksmiths, professional security consultants, and your local police crime prevention unit. All have experience with crimes to which you may be vulnerable, and expertise in how you can prevent them.

Security Consultants are extensively knowledgeable about the practical and financial aspects of internal security, and can objectively appraise your business's security loopholes to recommend appropriate corrective measures.

Business Associations, your local Chamber of Commerce, trade and other professional associations sometimes engage consultants to discuss security issues at regular meetings, usually when specific crimes threaten specific types of member businesses. You can discuss mutual security problems there to help you decide if you need to hire a consultant.

Police Crime Prevention Units provide office and business security checks, and give seminars or talks on personal and business security. Because they are usually oriented towards external crime, they may not be very helpful regarding your perceived internal security needs.

IDENTIFYING THE PROFESSIONALS

A suitable security services/equipment vendor will recoup your costs over time through increased equipment efficiency and security effectiveness.

To Choose an Equipment Vendor, check with other area businesses or companies in your industry for recommendations. Otherwise, interview at least three vendors: ask for bids to ensure fair market quotes and avoid inferior equipment purchases. Ask at least the following:

- How long have you been in business?
- Is your recommended equipment approved by UL (Underwriters Laboratory)?
- Will you identify, and may I contact, five current clients?
- Do you have liability insurance?
- Are you licensed/certified to provide the service/equipment you sell?

To Choose a Professional Security Consultant, again apply the advice above to obtain a comprehensive loss prevention scheme. Security consultants are generally objective and flexible in their approach to each project, so they rarely recommend only one manufacturer or vendor. A competent consultant will scrutinize your day-to-day operations function-by-function, to identify loopholes you and your managers are too "close" to see clearly. Although rates can range from $60 to $100 (and up) an hour, you will have wisely spent if your consultant identifies and ends a continuing internal diversion of assets.

2. BUSINESS SECURITY SURVEYS: *If You Have a Problem—What is It?*

WHO CAN DO A SECURITY SURVEY?

A security survey evaluates your external and internal security status to identify weaknesses presenting opportunities for criminal activity. You cannot necessarily control someone else's **desire** to commit a crime against your business, but you can reduce **opportunities**. Physical and internal security are equally important to you, your business, your employees, and your customers.

Your Police Department, often at no cost, can examine your physical premise, including your building(s), windows, doors, locks, lighting, fencing, alarms, landscaping, etc. The surveyor will then recommend steps to improve the quality of your external security measures.

A Private Security Consultant can survey your physical premise and can also address your internal security, i.e., policies and procedures controlling keys, cash, inventory, hiring practices, and information access.

A SECURITY SURVEY CAN. . .

- Provide an in-depth, on-site examination of your physical facility/property;
- Identify deficiencies or security risks (personal, physical, and information-related);
- Define protection needed;
- Recommend and facilitate the steps needed to minimize criminal loss opportunities.

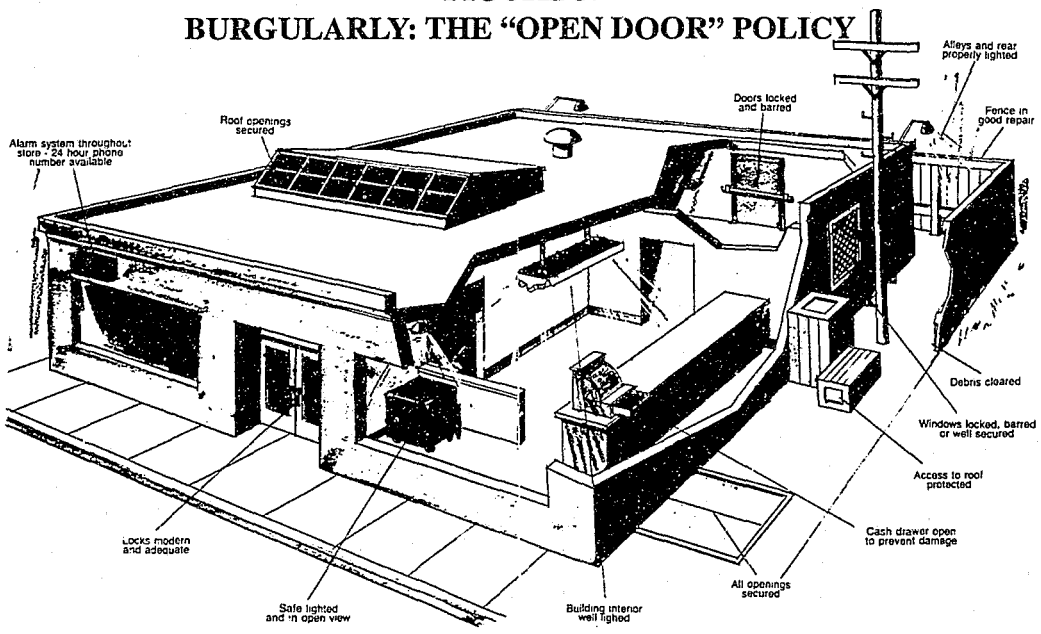
ESSENTIAL ASPECTS OF YOUR BUSINESSS SECURITY

- SUFFICIENT INTERIOR AND EXTERIOR LIGHTING IN GOOD WORKING ORDER
- CARD, KEYPAD, OR CODED ACCESS CONTROL SYSTEMS RESTRICTING AREAS TO AUTHORIZED PERSONNEL, AND CHANGED WHEN THOSE EMPLOYEES LEAVE YOUR BUSINESS
- SENSOR/ALARM SYSTEMS PROTECTING ACCESS POINTS (DOORS, WINDOWS/SKYLIGHTS, ETC.)
- STEEL GRATINGS OVER GLASSED ENTRY POINTS (IN AREAS HAVING HIGH RATES OF BURGLARIES OR VANDALISM)
- TAMPER-RESISTANT LOCKS ON ALL DOORS AND WINDOWS
- INTERIOR AND EXTERIOR TIME-LAPSE VIDEO RECORDERS AND CAMERAS TO RECORD SUSPICIOUS ACTIVITIES
- MIRRORS TO MONITOR YOUR PREMISE FROM VARIOUS LOCATIONS

WHAT A SECURITY SURVEY ASSESSES AND ANALYZES

- YOUR OVERALL BUSINESS ENVIRONMENT
- YOUR PREMISE'S GENERAL VULNERABILITY
- YOUR BUSINESS'S SPECIFIC VULNERABILITIES
- SPECIFIC SECURITY PROCEDURES AND/OR ENHANCEMENT
- SPECIFIC REMEDIAL HARDWARE (LOCKS, LIGHTS, ETC.)

FIGURE 5.
BURGULARLY: THE "OPEN DOOR" POLICY



3. LIGHTING: *Let's Shed Some Light Here*

LIGHTING CONSIDERATIONS

Good lighting in and around your business is a very cost-effective deterrent to crime. The elimination of even one dark shadow can dramatically reduce employees' and customers' perceptions of "gloom" and danger.

Lighting's technical terms—lumens, footcandles, refractors, coverage factors, etc.—need not intimidate you, but you should be aware of lighting considerations affecting your security. For example, high pressure sodium lights are both effective and low maintenance (versus metal halide, incandescent, or mercury lighting); "high mask" lighting evenly distributes over parking lots; floodlights are good for doorways; and a garage's indirect lighting can be enhanced by white-painted walls.

Even Light is *critical*: too intense light creates glare and reduces visual acuity at night. Your external security lighting scheme should *enhance* your existing lighting. Lighting sensors can also trigger additional lighting upon intrusions.

Reflectors *redirect* light and, properly utilized, provide additional effective, aesthetically pleasing light at little add-on cost.

Refractors, which can include glass bands, bowls, or globes, *control* light's direction by acting as prisms.

Color Rendition is affected differently by incandescent, fluorescent, mercury vapor, high-pressure sodium light sources, etc., and color perception under artificial versus natural light may have important security consequences.

EVALUATING YOUR LIGHTING

Your local utility company may offer a free evaluation service to answer your questions about your needs for security lighting (see Figure 6).

FIGURE 6.
SELECTED CHARACTERISTICS OF GENERAL TYPES OF LIGHTING SOURCES

CHARACTERISTICS	INCANDESCENT INCLUDING TUNGSTEN HALOGEN	FLUORESCENT	MERCURY VAPOR	METAL HALIDE	HIGH PRESSURE SODIUM	LOW PRESSURE SODIUM
Wattages (lamp only)	up to 3000	4 to 240	40 to 1000	400, 1000, 1500	70, 100, 150, 250, 400, 1000	35, 55, 90, 135, 180
Life (hours)	500 to 1,000	12,000 to 20,000	16,000 to 24,000	6,000 to 15,000	20,000 to 24,000	18,000 to 20,000
Lumens per watt (lamp only)	17 to 23	67 to 83	45 to 63	80 to 100	100 to 140	130 to 185
Color rendition	Very good to excellent	Good to excellent	Fair to very good	Excellent	Fair	Poor
Light direction control	Very good to excellent	Fair	Very Good	Very Good	Very Good	Fair to good
Source size	Compact	Extended	Compact	Compact	Compact	Extended
Comparative fixture cost	Low because of simple fixtures	Moderate	Higher than incandescent, generally higher than fluorescent	Generally higher than mercury vapor	High	Comparable to high-pressure
Comparative operating cost	High because of relatively short life and low lumens per watt	Lower than incandescent; replacement costs higher than HID because of greater number of lamps needed; energy costs generally lower than mercury	Lower than incandescent; replacement costs relatively low because of relatively few fixtures and long lamp life.	Generally lower than mercury vapor; fewer fixtures required, but lamp life is shorter and lumen maintenance not quite as good	Comparatively low; few fixtures required.	Generally the lowest, but application and coverage may raise costs above high-pressure.

4. CLOSED CIRCUIT TELEVISION (CCTV): *They're on Candid Camera!*

Understand the potential benefits of a closed circuit television (CCTV) system before you use it. For example, do not install cameras and monitors without assigning monitoring/recording activities; do not install CCTV where your customers expect privacy. Your security in these areas must depend on other measures. Advice from professionals and your own common sense will save money, increase business security, and avoid legal "backfires."

A CCTV system can monitor:

- Remote sites, such as vehicle gate openings;
- Sensitive areas, to include cash registers, vault access, etc.;
- Multiple locations simultaneously, using only one location or observer;
- Significant but infrequent events, like hold-ups or burglaries.

An effective CCTV system can secure you against both "insiders," employees and customers alike; and "outsiders," like burglars. Employees' "security awareness" will increase if you hide your CCTV cameras/monitors, while outsiders will avoid cameras that are visible. The system can be designed to meet your needs.

Cameras and monitors are relatively inexpensive. Your recorder may be expensive, since the number of heads and the time-lapse capabilities you need/want will determine your cost; however, they can be very helpful to your internal investigations. Exotic items now include matchbook-sized video cameras and "pin-hole" lenses hidden behind dropped ceilings, inside pencil sharpeners, or in other unusual places.

ESTIMATED COSTS FOR CCTV EQUIPMENT

CAMERAS	$ 150 - $ 400
LENSES	$ 150 - $ 450
MONITORS	$ 90 - $ 500
TAPE DECKS	$ 400 - $2,000

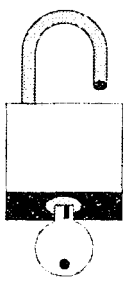
5. LOCKS AND OTHER HARDWARE: *Lock the Barn While the Horse is Still Inside*

DOOR CONSTRUCTION

Properly protected business doors will let you "survive." Most burglars enter through "weak" doorways. Think like a burglar: how would you get in?

Burglars kick through cheap, hollow-core doors, especially if strike plates, hinges, and frames are of poor commercial grade. Do not economize: choose metal, solid-core, or glass doors, all available in a variety of strengths, thicknesses, tints, tempers, wire-reinforcements, and laminations for all security purposes. Use only inside-opening hinges, and one-way screws.

LOCKS AND KEYS



Your primary security hardware, a maximum protection lock, is an electronic access control system. However, your exterior doors should at least have deadbolt locks, of which there are a variety:

- Single or double cylinder deadbolts;
- Mortise (commercial) deadbolts;
- Concealed header and threshold bolts;
- Rim-mounted deadbolts.

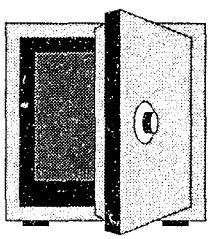
Keys are a common security failure, due to indiscriminate key assignment. Distribute keys only on a "need-to-have" basis. Numbering and stamping keys "DO NOT DUPLICATE" may give you some protection, but change critical locks when key-holding employees depart. Your locking system should include lock types you can change quickly and inexpensively.

Combination locks, which use numbers or other symbols, are generally more secure than key-locks, because there is no keyway access. However, change combinations on a regular basis, or at least whenever code-bearing employees leave.

SAFES

Your safe(s) should be:

- Certified fire- and burglar-resistant by Underwriters Laboratory. The UL approval rating is usually mounted on the inside of the safe's door;
- Embedded in concrete or bolted to the floor after removal of any wheels or casters. "Mobile" safes are usually "unsafe safes;"
- Attached to your security and safety alarm system;
- Located openly so that burglars cannot tamper with it privately.



Cost will depend on the safe's burglar-resistance. The longer it takes the would-be burglar to pry, chop, rip, or decipher the combination of your safe, the more it will cost. Only you can decide what type of safe you need and can afford. Prices can range from $300 to $12,000. Obtain advice on how to balance your investment against your risk.

OTHER HARDWARE

You can effectively protect windows, transoms, skylights, ventilation shafts, and air vents with iron screens, grills, and bars. However, what keeps criminals out can also keep your employees and customers in in the event of fire or other emergency. Avoid major liability claims by providing adequate exits; check all local, state, and federal building codes to ensure your compliance with safety and other standards before you install any physical security devices.

Your local police crime prevention unit can provide you with free information about doorway security hardware. Most can also provide you with a booklet entitled "Commercial Security," offering many low-cost or no-cost suggestions on how to secure your business against "outsider" criminals.

6. ALARMS: *"Things that Go Bump in the Night" (or Day)*

If your neighboring businesses are "alarmed" but you are not, the average professional burglar will prefer to burglarize your establishment. You should select an exterior (perimeter) and/or interior alarm system appropriate to your business security needs. There are two types of signal transmissions: *wireless*, using radio frequencies, transmitters, and receivers; and *wired*, using electromagnetic transmitters, low voltage, and hard-wire. These signals can be transmitted in several manners.

EXTERIOR (PERIMETER) ALARMS

Local Station Reporting triggers on-site audio and/or visual devices, to include sirens, horns, or flashing lights, alerting both intruder and immediate neighbors to the attempted invasion of your premises.

Central Station Reporting sends an audible or silent signal to your alarm company's monitoring station, which is often far distant from your premises. The station then notifies your local police or private security agency to respond. You may find it appropriate to combine a central station with a local alarm so that you deter the intruder at the same time that your security force is alerted.

Monitored Central Stations watch after-hour openings and closings, recording any unscheduled or unanticipated arrivals/departures; when warranted, it notifies police or employee monitors. It normally employs signals coded for selective types of events, like abnormal entries/exits, fire, robbery, burglary, etc., and usually causes fewer false alarms and consequent costs.

Unmonitored Central Stations usually cover only fire, robbery, and burglary events, because its uncoded signal/notification normally requires police, private security, or central station emergency response.

INTERIOR ALARMS

To protect against your perimeter alarms being bypassed or failing, you can customize your system with one or more of five basic types of interior sensing devices:

An Audio System reacts to unusual noises, transmitting them to a monitoring control center. Some systems amplify the noise, which itself triggers another alarm.

A Microwave System reacts to motion generated within a defined electromagnetic field. As this system penetrates glass and wood, it is best installed in areas completely enclosed within steel and/or concrete. This will help to prevent false alarms caused by passing vehicles or persons.

A Photoelectric System detects anything breaking its beam either inside or outside, although a knowledgeable intruder can bypass it. The beam travels in a straight line so furniture or other normal office equipment can block it.

An Ultrasonic System triggers an alarm when its soundwaves are interrupted by movement within the protected area. Soundwaves can also be blocked by furniture and normal office equipment, but because soundwaves are everywhere, an intruder cannot avoid disturbing the field.

A Passive Infrared System detects changes in a protected area's normal radiation/temperature environment, such as a person moving through the field of coverage. It can monitor large, open areas and cannot be detected by an intruder, but it is not an alarm signal, only a receiving/recording device.

SELECTING AN ALARM COMPANY

Talk with several alarm companies, or at least consult your security surveyor, before you commit. Address the following issues:

- Ask the Better Business Bureau about the company's business complaints;
- In coordination with your insurance carrier, request proof of liability insurance against system failure; contact your local police for the company's "false alarm" rate, and its and your liability for false alarms;
- Discuss with the alarm company their sales volume and size of their work force;
- Require UL-approved alarm equipment and central station;
- Ask your local building inspector to inspect your alarm installation for compliance with all applicable codes.

ALARM COSTS

You must balance your alarm system investment costs against your risks. The following are some estimated costs current at the time this *Guide* was issued:

ESTIMATED COSTS FOR ALARMS

LOCAL ALARMS	
• **Installation:**	**$ 350 - $ 900**
• **Monthly payments (lease and maintenance):**	**$ 40**
SILENT ALARMS	
(perimeter and interior detection systems)	
• **Installation:**	**$ 500 - $ 2,000**
• **Monthly payments (lease and maintenance):**	**$ 30 - $ 50**
SUPERVISED SYSTEMS	
• **False alarms:**	**$ 20 - $ 35**

FALSE ALARMS

Because police respond to too many false alarms, many communities have laws regulating false alarms. Urban alarm calls account for approximately as much as 10% of all calls for police service; of those, at least 90% (and possibly more) are false alarms due to failure to adhere to standard "turn-on/turn-off" procedures, improper installation/maintenance, and failure to inform employees of proper procedures.

Review the cause of every false alarm so you can take proper preventative actions. Your alarm company is responsible for any deficiencies in installation or maintenance; this condition should be part of your contract with the company. Persistent and undetectable false alarms should alert you and your alarm company to re-evaluate and possibly reconfigure your alarm system to remove the source of the false alarms.

7. ACCESS CONTROL: *Is the Horse In Your Barn?*

You risk major loss if you do not protect your *assets* by limiting *access* to your premises. Access control systems can be expensive, but a proper analysis of your access control needs can:

- Prevent the installation of an improperly designed or poorly planned system;
- Ensure system flexibility, recordkeeping and notification capabilities, and physical integrity;
- Ensure your vendor's capabilities.

ACCESS CONTROL EVALUATION

All access control surveys should address your specific needs and identify appropriate devices and/or construction (e.g., do your doors need "card readers," alarms, or emergency access devices?). Access control can include any combination of the following:

- Card readers;
- Voice identification;
- Fingerprint identification;
- Eye identification;
- Security personnel.

You should become familiar with many technical factors that may be important to your access control plan:

- Do you need magnetic strips (Wiegand) or proximity-type cards?
- Do you need slot-, insert-, or proximity-type readers?
- Does the proposed system use 220- or 100-voltage; does the reader use 12- or 24-voltage?
- Is major construction required for your access doors and/or jambs?
- Is the card access system equipped with alarm points?
- Does the system have reverse polarity capability, to keep it operating even if a "reader" fails?
- Can the system transmit data by modem from remote areas to the central processing computer?
- How many card readers, modems, and cards do you need, and can your system handle them?
- What will new and replacement cards cost?
- Can the system be maintained via emergency power? Do you/they have an emergency power source, and how long can it back-up your primary power source?
- What is the system's procedure if the central processing computer fails?
- What is the system's maintenance needs and availability? How experienced are the maintenance personnel? What is maintenance's turn-around time?
- What is the total maintenance contract cost? How much will each maintenance item cost?

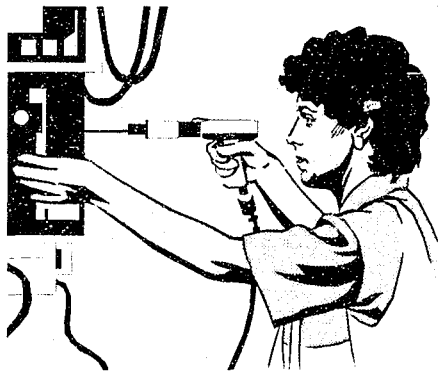
FLEXIBILITY

Given employee turnover, install an access control system that allows you direct control over entry into specific areas. For example, a security intercom system can allow you to "buzz" people into your office, or to see and talk to them. It should be adaptable to meet future growth in your work force or changes in your business needs.

RECORDKEEPING AND NOTIFICATION

Your access control system, which can also be used in place of time cards, should be able to validate the identities of all persons using the system, and to identify and record individual entries, or attempts, into protected areas. Ideally, it should allow you to limit or reduce days and/or times when personnel are permitted access to protected areas, and should also be able to notify you, via some form of alarm and accompanying documentation, whenever any alarm point or access card has been compromised or tampered.

PHYSICAL INTEGRITY



You need a tested, rugged, and reliable access control system able to withstand substantial physical force, protected from casual electronic manipulation, and reputable for easy maintenance, service, and repair.

SELECTING YOUR VENDOR

After you identify a system meeting those criteria and your needs, contact available vendors and provide them with your card access specifications (before they visit your facility) for the vendor's review during his on-site tour. After selecting your vendor, carefully monitor all construction and installation work until completion. Close communications with your vendor, then and throughout your maintenance contract, will be valuable as you update and upgrade your access control system.

D. GUARDS AND SECURITY SERVICES

A Guard In Time May Save. . .

If your security problems are severe, a security analysis, consultation with your local police department, and informal discussions with other business owners in your area and industry will help you decide if you need a security guard service to protect your assets, employees, and customers.

HOW TO SELECT A GUARD SERVICE

The guard service you select should meet the following criteria:

A Good Public Relations Image. Guards who help control access to your business, and thus have contact with your customers, must present a professional appearance and have good "people" skills.

Good Skills, Training, and Quality Control. A good guard service will provide guards trained in interpersonal communications, professional ethics, report-writing, CPR, first aid, telephone skills, etc. The service should work with you to prepare written post security orders and procedures to cover anticipated situations, such as observed thefts, apprehension of shoplifters, power outages, unauthorized intrusions, and other emergencies. The service should also provide a continuing training program for guards and their line supervisors, as well as a management/operations audit survey program.

Good Supervision. You should require a 24-hour emergency response to any security problem reported. The service should respond immediately to correct the problem and then provide you with written recommendations about preventing similar problems in the future.

Sufficient Liability Insurance. The service should have at least $1 million in general liability insurance.

OTHER CONSIDERATIONS

You must decide if you want uniformed or plain-clothed, armed or unarmed guards. Cost is also a significant factor: a guard providing 24-hour daily protection represents 168 hours per week at a cost of $7 to $22 per hour. Given these considerations and the selection criteria above, you should be able to choose a security service that will protect your business and provide a return on your investment.

CHECKLIST FOR CONTRACTING WITH A GUARD SERVICE

- Determine the security responsibilities to be performed;
- Prepare written security specifications, including hours of coverage, manpower and equipment needs, insurance requirements, and any special work requirements;
- Contact several qualified guard services, provide them with your security specifications, request them to attend a bidders' conference, and require them to provide you, in writing, with:
  - their corporate background, qualifications, and experience; names of officers and board members; current financial status, to include any current insurance liabilities affecting their coverage;
  - their selection, training, and promotional policies and procedures, including drug testing and background checks;
  - their top 5-8 client names and addresses.

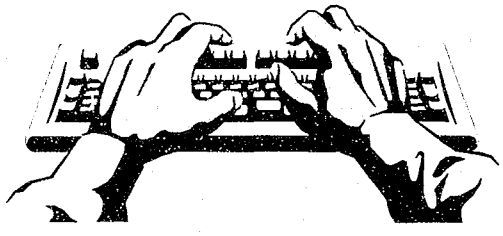
E. COMPUTER-RELATED CRIME

Why You Should Be Concerned About Hackers, Viruses, and Disgruntled Employees

YOUR COMPUTER IS AT RISK

Computers ("informational technology") have introduced new variations on traditional forms of internal theft. Why computer-related crime has "boomed" in incidence, seriousness, and sophistication is not known, but it has recently caused unprecedented economic problems, from electronic funds transfer fraud to inventory loss.

Annual dollar losses to computer-related crime is only estimated at $3 to $5 billion, because commercial victims (including large and financially-sound businesses) are usually unwilling to report losses. Small businesses are not the sole victims of computer-related crimes, but if your small business has few resources and only one or two people involved with your computer system, computer security experts say you may have difficulty in recovering from computer-related losses. Take a no-nonsense approach to computer and information security: adopt and follow practical security measures to discourage theft and to provide yourself with reasonable protection against intentional damage, fraud, and other hazards.



Typical Offenses. (1) A disgruntled employee leaving your business erases selected employee files and changes employee passwords; (2) an employee uses your computer system to clear personal and friends' charge accounts.

PREVENTING COMPUTER-RELATED CRIMES

Computer abuse, computer fraud, and computer crime are *legally different*. However, this *Guide* **considers computer-related "misuse" to be any illegal act requiring computer technology knowledge.**

Do not be intimidated by your computer's operations and powers. Because it increases your efficiency and effectiveness, your computer must be protected, cared for, and used correctly. The following policies/procedures will help you reduce your risk of being victimized by a computer-related crime.

Provide Optimum Physical Protection and Limited Access. Site location(s) away from heavy traffic areas, preferably in access-controlled area(s). If you must allow general computer access, bolt the equipment to an immovable object.

Mark and Inventory Your Equipment. Record and store, though not in your computer, all computer and peripheral equipment identifying numbers. Physical identification on your equipment may prevent its theft, and will improve the chance of its return. Contact your local police department about "Operation Identification."

Hire and Train Competent Employees. Your legitimate data processing staffers with authorized access may be tempted to compromise your system. Conduct thorough background investigations of potential hires to ensure "fitness" for the position; "bond" persons having fiduciary responsibilities; involve all employees in identifying and correcting potential security dangers.

Divide Responsibility. Do not make any one person responsible for computer security. Wherever possible:

- Assign two people to computer projects;
- Rotate operational personnel, reassigning computer access as appropriate;
- Restrict access to computers, programs, documentation, sensitive forms, checks, etc.

Establish a Computer Use Policy. Formulate policy regarding business (and/or personal)

computer use. Orient new employees to your policy, and require a regular review of it (e.g., at employees' annual evaluation).

Require Employee Passwords. Prohibit common dictionary words, often easily compromised by "hackers," and periodically change the confidential alpha-numeric combinations used.

Regularly Monitor/Audit. Look for improved methods of authenticating users and terminals ("port"-protection). Certain software programs can record and monitor user access and identify unusual activity, even after hours and on weekends. Tell employees that you audit, but do not discuss your actual audit procedures.

Adopt and Follow Accepted Procedures. Do not wait to "discover" that your "back-up" data will not recover your system because a "virus" has destroyed it or a hacker has stolen it. Regularly "back-up" your data, programs, and documentation; store them securely, away from users, and randomly verify their reliability.

Protect Vital Information. Shred discarded paper copies of computerized account and credit card numbers, PBX, voice mail codes, etc. You may have applicable and protected copyright, trade, or confidentiality agreements. Do not let your trash become someone else's treasure!

KEY COMPONENTS TO A BUSINESS COMPUTER PLAN

- POLICIES PROHIBITING UNAUTHORIZED USE OF COMPUTERS
- BUILDING SECURITY PROCEDURES LIMITING ACCESS TO COMPUTER EQUIPMENT
- STANDARDIZED DATA AND SOFTWARE SECURITY PROCEDURES
- COMPUTER SECURITY AWARENESS TRAINING FOR EMPLOYEES
- EMPLOYEE AWARENESS (SIGNED FORMS) OF POLICY AND RECEIPT OF TRAINING

IF VICTIMIZED—WHO SHOULD YOU CALL?

You should report any computer-related crime to your local police department. However, you may be reluctant to report because:

- You may not have discovered the crime within required timeframes;
- You may be unsure about employee privacy or other rights protections;
- You may fear creating an undesirable working atmosphere by installing procedures perceived as "too stern."

While business victims have reported unsatisfactory police and prosecutor response to their computer-misuse complaints, you—the victim—are still the police's best source of assistance and prosecutors are becoming more experienced with computer-related crimes.

Private investigators are hired by many businesses to investigate computer-related crime inside their organizations. This allows the owner to have the investigation completed without publicity. These investigations usually end in the dismissal of an employee without criminal prosecution. All too often, the dismissed employee will be hired by another employer, who then becomes the next victim.

F. INVESTIGATIONS

To Catch a Thief. . .

TO CALL—OR NOT TO CALL—THE POLICE

What should you do when you receive—directly, or indirectly via anonymous letters, telephone tips, etc.—*information concerning* internal thefts, other illegal acts, or otherwise business-threatening activities? Your own observation may be incomplete or inaccurate, and information given you may often be a half-truth complicated by the passage of time and biased by the messenger's prejudices. Nonetheless, you often must decide what to do after you have received this type of information.

Your police department has manpower limitations, which is why you may find it difficult to involve them in complicated or comprehensive investigations. **Report the theft anyway.** The police are not unwilling to assign an investigator, but the more stringent local government budgets in the 1990s has made it more difficult for them to follow up on your business property crime.

Even if the internal crime threatens your business's "life," only you—alone—can decide how to handle it. This *caveat* applies especially to perceived or alleged substance abuse problems in your workplace and work force. Contrary to popular opinion, your local police department often cannot place an undercover officer inside your work force. You should address substance abuse issues before a police investigation becomes necessary.

THREE ELEMENTS OF AN INVESTIGATION

The three elements common to any investigation include: the purpose of the investigation; the investigator; and the subject to be investigated. It is paramount to decide the purpose of the investigation before you decide how you are going to accomplish that purpose. Some common goals of investigation can be:

- To criminally charge the employee;
- To effect insurance recovery (internal theft);
- To receive restitution;
- To eliminate the problem without pressing charges;
- To avoid adverse publicity;
- To internally publicize a successful investigation.

Next, you need to decide who should pursue the investigation. Police involvement may garner adverse publicity, but it could also impress your employees with the seriousness of the offense under investigation. Your options for the investigating agency include:

- You;
- Your internal security personnel;
- The police;
- A company supervisor;
- A licensed private investigator.

KEY FACTORS WHEN YOU INVESTIGATE AN INCIDENT

- GATHER ALL AVAILABLE FACTS
- CONDUCT THOROUGH INTERVIEWS AND DOCUMENT ALL RESPONSES
- ATTEMPT TO CORROBORATE INFORMATION RECEIVED
- DECIDE WHO TO CONTACT SHOULD YOUR INVESTIGATION REACH THE CRIMINAL CHARGING STAGE

Should you decide to be the investigator, assess your ability to be objective, given your proprietary interest in your business, and your personal knowledge of your employees. Do not sacrifice thoroughness and accuracy because you believe you "know" the offender; doing so may set you up for a "wrongful termination" action.

An in-house investigator may be a luxury for your business. However, if you have that capability, do not assume all security personnel are capable of conducting a thorough, accurate investigation. Many inquiries have foundered by relying on untrained in-house personnel.

TYPES OF INVESTIGATIONS

Undercover Investigations. An operative, usually obtained from a specialized, licensed private investigative company, is placed in your work force posing as a "regular" employee for 6 weeks to 6 months or longer. Many large companies maintain "permanent" intelligence operatives to monitor the pulse of the employee environment.

The most sensitive action is placing the operative without arousing co-worker or supervisory suspicions. Inform only the personnel supervisor of your purpose (and only if necessary). Screen/recruit as with all other new hires; if layoffs or job freezes cannot justify a new hire, "invent" a contractual or temporary position. To ensure the operative's objectivity, do not "point" or "direct" him/her towards any single employee, group, or department.

Once in place, your operative should mail daily reports to you or your representative at a home, or other secure address to protect the integrity and security of the investigation and the identity of the operative. Unless your operative is "expert" in a particular subject, the reports should be without bias and should cover all topics you designate, including:

- Morale problems;
- Supervisory failures;
- Safety issues;
- Substance abuse;
- Theft;
- Rumors.

Do not discuss your operative's reports with anyone unaware of the investigation. Do not react in "knee-jerk" fashion to the report: you can compromise the investigation by alerting employees to management's "interest" with sudden or unexplained transfers, demotions, firings, or increased supervision. If possible, take remedial action only after the investigation is complete.

Specific Incident Investigations. These should be conducted when you have a problem such as:

- Major theft;
- Repeated petty thefts;
- Employee abuse of leave;
- Fraudulent Worker's Compensation claims.

Such investigations should have well-defined starting points, clear-cut goals, and finite endings. If you use an outside agency for this purpose, clearly state your goals and your budget allocation. Costs are currently $35 to $55/hour for routine investigations, and up to $75/hour for complex frauds or other white collar crimes.

HIRING AN AGENCY

Finding an Agency. If you determine that an outside investigator is appropriate for your situation, the problem becomes one of identifying which agency to hire. We suggest you turn to your legal counsel or contact other companies within your industry for a referral to a competent and professional investigative company. "Word of mouth" is often more effective than identifying an agency by the size and attractiveness of the display ad in the classified section of your telephone directory.

Selecting an Agency. It is extremely important the outside investigator be familiar and experienced with your type of business and clearly understands your goals in this investigation. For example, if you merely want to make an "impression" on your employees, do not hire an investigator who is intent on identifying and prosecuting "perpetrators."

You should be certain the outside investigative firm is properly licensed and insured for the type of work you want them to perform. Unprofessional, sloppy, or itinerant investigators frequently find it impossible to obtain liability insurance. To a degree, you can protect yourself by insisting on a *Certificate of Insurance* from their insurance company. This certificate will ensure that you will be notified if the investigative company has their policy canceled.

Supporting an Agency. Investigations can involve the use of undercover operatives, CCTV equipment, surveillance, interviews, document examinations, and/or complex reviews and audits of your financial records. Very few investigative agencies are experts in all of these techniques. Be certain that the agency you hire is prepared to seek assistance in those specialized areas of investigation where they lack the necessary competence.

It is advisable to keep your attorney abreast of any investigation, particularly if a decision may be made to discipline, terminate, or prosecute any employee. In general, no permanent action should be taken against an employee until the investigation is completed and all facts are known.

If it appears appropriate to prosecute and involve the criminal justice system (i.e., police, prosecutor, etc.), then the investigative agency should be required to contact the police/prosecutor to clarify the roles, responsibilities, and procedures of each agency. You want to know what your investigative agency will be responsible for during the criminal investigation and preparation for prosecution.

POLYGRAPH EXAMINATIONS

You may request an employee to submit to a polygraph examination in the course of investigating a workplace incident causing economic loss, but only if:

- The employee(s) had access to the property, or was involved in the incident under investigation;
- You have "reasonable suspicion" of the employees' involvement;
- You provide the targeted employee(s) with a written statement of the company's reason(s) for investigation.

WHAT YOU SHOULD KNOW ABOUT THE USE OF POLYGRAPH EXAMINATIONS

- A POLYGRAPH EXAMINATION SHOULD NOT BE USED WITHOUT LEGAL ADVICE
- YOU CANNOT TERMINATE AN EMPLOYEE FOR REFUSING TO TAKE A POLYGRAPH EXAMINATION
- YOU CANNOT TERMINATE AN EMPLOYEE SOLELY ON POLYGRAPH RESULTS
- YOU CANNOT GIVE POLYGRAPH EXAMINATIONS TO PROSPECTIVE EMPLOYEES

Dealing with Targeted Employees. Do you confront him/her? Do you demand restitution or return of goods? Should you seek criminal charges or fire the employee? Your basic responses should include:

- Providing the employee with an opportunity to explain the incident/situation (but expect, usually, a general denial);
- Presenting your findings in a matter-of-fact manner;

- Avoiding accusatory statements.

Employee Rights. If you inadvertently deprive employees of specified rights under the law, you may be subject to legal proceedings. Inform your attorney of any investigations, especially those which may lead to employee discipline, termination, or prosecution. Take no "final" employee action until the investigation is completed and substantiated. Seek legal advice before making even the mildest accusation.

KEY CONDITIONS WHEN INTERVIEWING EMPLOYEE(S)

- EMPLOYEE(S) SHOULD BE "ON THE CLOCK"
- INTERVIEW(S) SHOULD TAKE PLACE IN AN UNLOCKED ROOM
- INTERVIEW(S) SHOULD CONFORM WITH EMPLOYEE CONTRACT OR UNION AGREEMENT
- EMPLOYEE(S) MUST FEEL FREE TO TERMINATE INTERVIEW(S) AT ANY POINT

SURVEILLANCE AND SEARCHES

- COMPETENT LEGAL ADVICE IS ABSOLUTELY NECESSARY
- MOST COMPANY PROPERTY SEARCHES ARE PERMISSIBLE
- MOST PERSONAL PROPERTY SEARCHES ARE NOT PERMISSIBLE
- SURVEILLANCE OF GENERAL WORK AREAS IS PERMISSIBLE
- SURVEILLANCE OF SPECIFIC WORK AREAS MAY REQUIRE NOTIFICATION
- SEARCH PROCEDURES SHOULD BE ADDRESSED IN COMPANY POLICIES
- SEARCHES OR SURVEILLANCE SHOULD BE CONDUCTED ONLY ON REASONABLE CAUSE

G. INTERACTION WITH THE POLICE AND THE CRIMINAL JUSTICE SYSTEM

Working Together Can Make a Difference

To protect your business, you should know and interact with your local criminal justice system. Your most frequent contact with police will be the patrol officer responding to your calls for service and the police detective who conducts any subsequent investigation. Although contact with your local State's Attorney or District Attorney will be substantially less, you will have opportunities to work with them because police clearance rates are higher in cases of internal theft (i.e., the "pool" of suspects is smaller).

WORKING WITH THE POLICE

Police are generally unenthusiastic about internal theft cases because their limited resources cannot sustain lengthy or complicated investigations (e.g., embezzlement, fraud, etc.). They have also been "burned" by companies who initially welcomed their assistance, but then refused to prosecute the subsequently identified perpetrator. However, your local police can assist you and your business with a number of preventive and investigative services.

Get to know your local precinct/district commander or chief of police to become familiar with the services currently offered in your community. Your police department's crime prevention package includes brochures identifying critical information only they can provide; likewise, you can work with them by providing "current crime environment" information that only you and other local businesses have.

Prevention. Most police departments have excellent crime prevention programs. As part of their focus on "external attack," some specifically target businesses (as previously mentioned in this *Guide*), e.g., providing information about existing crime in your area (gangs of shoplifters, patterns of commercial or retail burglaries or robberies, etc.). Your local crime prevention officers can also provide assistance with your internal theft prevention program.

Do not discount the deterrent factor added by the omnipresence of uniformed patrol officers. Get to know them; exchange names; talk about your concerns before you uncover an acute problem. The better your patrol officers know your area, the better they can plan to protect it and you.

Emergency Response. Call your police department's emergency telephone ("911" in most communities) whenever you or your employees witness a crime or suspect a crime being planned (whether internal or external).

Use your police department's guidelines to observe and record as much information as possible for the responding officer, (e.g., identity data about the person(s) involved; description(s) of property stolen; location(s) the perpetrator may have been (e.g., point of entry, areas invaded, etc.).

External Crime. Having taken our advice to get to know your police precinct/district commander or chief of police, you can anticipate their response to business victims. At minimum, you should be informed of any major changes in case status (e.g., recovered property, suspect(s) apprehended, etc.). On your part, inform the assigned officer or detective of any additional stolen items, suspicious persons, possible suspects, etc. Affirm your intention to cooperate with case prosecution (e.g., talk with the prosecutor, attend court, etc.).

Internal Crime. Work closely with your police when you suffer or suspect internal losses due to employee theft or workplace drug use. Begin by establishing appropriate company policies regarding:

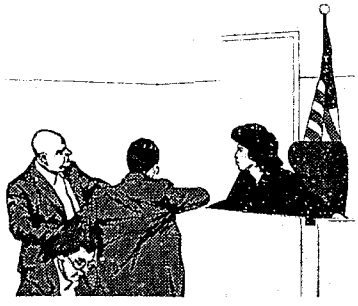
- When and why police will be called;
- Who will make the first, critical call on your behalf;
- What the company will provide to the police;

- How you and your company will respond to investigation(s) and subsequent prosecution(s).

Before implementing such policies, seek advice from your police department and prosecutor about your needs regarding the nature and extent of police intervention and joint police/prosecutor investigations.

WORKING WITH THE PROSECUTOR

Commit yourself to a clearly-defined policy to proceed with prosecution, whether civil or criminal. However, your company policy should not mandate prosecution, because you need to evaluate the merit of pursuing each case in light of potential costs. Your prosecution policy should also specifically avoid using the criminal court, especially District (lower) Court, as your collection agency or arbiter. Should you initiate criminal prosecution solely to cancel a debt or to force settlement of an internal dispute, the prosecutor will take a dim view of both you and your complaint, and may summarily dispose of your case, sometimes before a court date is set.



How and When to Prosecute

- Criminal versus civil remedies. This will be your most difficult decision in cases of "insider" theft or fraud. Civil action often will not be an option if criminal activity (particularly drug involvement) is uncovered during the investigation.

- Potential expenses. Consider your direct and indirect expenses in pursuing any prosecution. Weigh the various cost factors, including your time gathering and preserving records and information, and potential income/profits lost should you or your employees go to court on a business day.

Initiate and Maintain Contact with Your Prosecutor. A common complaint about the criminal justice system—and the prosecutor in particular—is the failure to communicate case status, especially postponements or dropped charges. However, most prosecutor's offices now have Victim/Witness Assistance Units acting as your liaison with the prosecutor and your clearinghouse for case status updates. Absent such a unit, be sure to initiate and keep open communications. Contact the assigned prosecutor immediately upon notification of a trial date or hearing, giving your name, address, and telephone numbers. Offer to coordinate interviews and court appearances when your employees are summoned as witnesses. By doing so, you may have more "say" in hearing or trial date scheduling. Tell the assigned attorney that you can assist in obtaining a conviction only by being kept informed, and that the schedules of you and your employees should be considered by the court when setting new dates.

Coordinate Schedules. Your business cannot afford time lost from work or reduced productivity due to extended time spent in court. Minimize actual dollar losses by maintaining open communications with your prosecutor, designating a "contact person," and informing the prosecutor of prospective employee work and leave schedules. Also, consider extending or arranging for employees' administrative or paid leave, or group transportation for all necessary court appearances. Use any "delay" time to continue your own internal investigation: some of the most convincing evidence is uncovered immediately before trial.

Do Not Become Discouraged or Impatient. The criminal justice system truly "grinds

slowly," because courts and prosecutors are inundated. Your case will be delayed at some point. You will successfully interact with the justice system if you and your prosecutor aggressively and diligently try to accommodate each other's interests. **Your key to success is a righteous concern, tempered by patience, understanding, and a willingness to adjust schedules.**

YOUR PROSECUTION

Keep Records. It is as important to keep good records for your criminal prosecution as it is for your business transactions, productivity, and output. Because memories of events begin to fade after only days, you must record timely, complete, and accurate information about witnesses, business records, statements, and pertinent background items.

Be Prepared and Available. As witness to or victim of the crime, your support of the prosecutor will be critical, particularly for internal crimes where seemingly mundane details and ordinary business operations become important. For example, the prosecutor may need on-site observation of your offices or file arrangements, or may need knowledge of your computer, transaction, or inventory systems to understand how the crime was committed. Ensure that employees/witnesses know your need for their cooperation with the prosecutor.

Identify the Crime's Impact on Your Business. Many states have adopted the use of *Victim Impact Statements* in the sentencing process. As the **victim**, you should be prepared to present the **impact** of the crime in a logical and cogent **statement**, accounting for your financial losses (including actual damages and man-hour productivity losses incurred in support of the investigation and prosecution), as well as the emotional and psychological effects on you and your employees.

Upon conviction, some jurisdictions may ask you to suggest the form of punishment or an acceptable alternative to incarceration. Community service, even in connection with your business, may be fitting in certain cases. Be prepared to offer options to the prosecutor and the court.

Part IV. CONCLUSION

What Should I Do Now ?

Let us re-examine the three principles that must be present before deviance will occur.

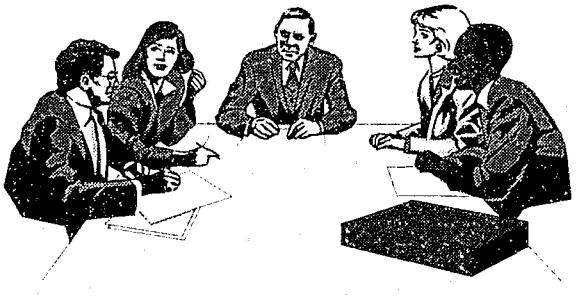
(1) The Deviant Act Must Be Motivated by One or More Causative Factors.

What Can I Do to Prevent This "Motivation"?

First: Do not hire employees who have documented or demonstrated repeated acts of deviance *prior* to applying to your company. Screen prospective employees via background investigations and/or drug testing.

Second: Do not precipitate employee dissatisfaction by paying substandard wages or requiring unreasonable workhours (particularly if you do not work those hours). Create an environment which fosters your employees' belief that your company cares about them personally, beyond the bottom-line profit.

Third: Communicate openly and frequently with your managers and encourage them to communicate with their subordinates and front-line employees. Address all issues causing morale problems quickly and effectively. Encourage teamwork at all levels to make employees feel empowered and involved with company goals.



You cannot eliminate all factors causing employee deviance. However, hiring good people and keeping them team-motivated will reduce your risk of work force deviance.

(2) An Opportunity to Commit the Deviant Act Must Be Present.

How Can I Reduce This Opportunity?

You must emphasize **PREVENTION!** Do not send "uncaring" messages, via sloppy inventory procedures, unlocked critical areas, unprotected but important proprietary information, or your own failure to follow security policies and procedures.

Convey your personal commitment to an environment conducive to security. If you follow this advice, you will have greatly reduced the opportunities that deviant employees have to harm the company.

Once you hire good people, make them part of the team by prudently creating a suitable business environment emphasizing **PREVENTION.**

(3) There Must Be a Perceived Absence of Formal Controls and Sanctions.

How Can I Avoid This Situation?

Formally document your expectations of employee conduct at the workplace. Your employees will not—indeed, cannot—respect your policies if they have not been officially informed. Do not dictate policy and then ignore violations. Sanctions must be applied uniformly throughout your business at all levels (e.g., a manager receiving a "slapped wrist" for an offense causing another's termination or suspension will immediately lower morale and encourage disaffection and deviance).

Compliance checks to reveal misconduct may take many forms, including hotlines, audits, undercover investigators, etc. Once you have defined expected conduct, you need to define sanctions appropriate to the misconduct, from referral to an Employee Assistance Program to reassignment or termination.

Your "bottom-line" depends to a great extent upon your understanding and allegiance to the three principles stated above, and exemplified below:

- Hire the "right" people;
- Treat your employees with respect;
- Communicate with your employees;
- Tell your employees how you expect them to conduct themselves;
- Devise methods to monitor compliance with your standards;
- Devise appropriate sanctions for improper or deviant behavior; and
- Apply sanctions uniformly.

You should take to heart the observation made by Clark and Hollinger, in *Theft by Employees in Work Organizations*:

> "We found that those employees who felt that their employers were genuinely concerned with the workers' best interest reported the least theft and deviance. When employees felt exploited by the company or their supervisors (who represent the company in the eyes of the employees), we were not surprised to find employees most involved in correcting this perception of inequity or injustice by acts against the organization."

John P. Clark and Richard C. Hollinger, *Theft by Employees in Work Organizations: Executive Summary* (National Institute of Justice, Washington, DC), 1983.

PART V. REFERRALS AND RESOURCES

CRITICAL PROBLEMS—AND ANSWERS

PROBLEM: ***"I have received several anonymous complaints about narcotics abuse, and one employee overdosed while on the job."***

Discussion: Consider comprehensive interviews with employees, one-on-one, to solicit more complete information. If the problem seems widespread, consider contacting the police or a private security company. A private security undercover placement may be helpful (see Part III-F, Types of Investigations and Part III-G, Working with the Police). Devise a written drug policy, which each employee should review and sign (see Part II-B, Your Company Policy and Program).

Resources:

- Local police department "drug resistance" unit;
- Local drug abuse program coordinator;
- Corporate legal counsel; and
- Private security services.

PROBLEM: ***"I have several employees exhibiting strange behavior before drug tests, but they all tested negative!"***

Discussion: Make certain that employees are escorted by supervisory personnel if tests are conducted off-site. Build controls into your on-site testing to ensure that the fluid samples are actually collected from the suspected employees (see Part II-B, Designing and Implementing a Drug Testing Program).

Resources:

- President's Drug Advisory Council;
- Local drug abuse program coordinator; and
- National Institute on Drug Abuse.

PROBLEM: ***"I am experiencing both high turnover and poor performance from our newest employees."***

Discussion: Consider instituting one or more of the methods to screen potential employees (see Part III-A-1, Pre-Employment Screening).

Resources:

- U.S. Department of Labor;
- Equal Employment Opportunity Commission; and
- American Personnel Association.

PROBLEM: ***"My business has been plagued by a recent rash of bad checks accepted by my employees."***

Discussion: Institute a comprehensive training/awareness program to motivate your employees to help you protect corporate assets (see Part III-A-2, Alert and Conscientious Employees, and Part III-B-2, Checks and Credit Cards).

Resources:

- Local police department crime prevention unit.

PROBLEM: ***"I have received several anonymous calls warning me that company products are being sold 'on the street,' outside of normal channels."***

Discussion: Carefully check inventory control procedures to identify areas of vulnerability (see Part III-B-1, Causes and Controls). Develop a telephone checklist to solicit as much information as possible should the anonymous caller(s) call again. Initiate an investigation, based on existing information, through your local police department, private security firm, or internal resources (see Part III-F, Types of Investigations and Part III-G, Working with the Police).

Resources:

- Local police department;
- Private security firm; and
- Your private security firm.

PROBLEM: ***"My business premise has been broken into four times within the past month. Other companies in the area do not seem to be having the same problem."***

Discussion: Schedule a security survey for your building to ensure that you are adequately protected at your geographical location (see Part III-C, Target Hardening, and Part III-C-2, Business Security Surveys).

Resources:

- Your local police department crime prevention unit; and
- Private security consultant.

PROBLEM: ***"Each week, I am losing increasingly large amounts of cash from my register."***

Discussion: If you have carefully screened your employees, review your cash handling procedures (see Part III-B-2, Cash Registers) and areas of vulnerability (see Part III-B-1, Causes and Controls).

Resources:

- Private security consultant; and
- Local retail merchants association.

PROBLEM: ***"I was recently approached by a person who said he installs alarms and circuit TVs 'on the side.' He said he's 'moonlighting,' but I can save 25% if I let him install the equipment."***

Discussion: Beware that many "moonlighters" operate without insurance and often are "drifters." If so, you are often left to deal with service and equipment problems (see Part III-C-6, Selecting an Alarm Company).

Resources:

- Better Business Bureau;
- Local Attorney General's Division of Consumer Protection;
- Private security consultant; and
- Your local police department crime prevention unit.

PROBLEM: ***"My company computer system was 'compromised,' and we were billed over $15,000 for unauthorized long-distance telephone calls. What should I do?"***

Discussion: Review your written computer security procedures, emphasizing your password system(s), division of responsibilities, and system audits (see Part III-E, Preventing Computer-Related Crime). Report all computer-related crimes to your local police department; you can also hire a private investigator (see Part III-E, If Victimized—Who Should You Call?).

Resources:

- Local police department;
- U.S. Secret Service; and
- Computer security consultant.

PROBLEM: ***"Three weeks ago, I caught an employee stealing, obtained a verbal confession, and arranged for his/her restitution to my company. I then fired the employee. I have not received any restitution to date—what can I do?"***

Discussion: You may have closed some of your options by negotiating with the employee without having first involved law enforcement professionals (i.e., filing criminal charges). They may now view this as only a civil matter, and may advise you to file a civil suit against the employee (see Part III-F, To Call—Or Not to Call—the Police, and Part III-G, Working with the Police).

Resources:

- Corporate attorney;
- State's Attorney's Office; and
- Local police department.

PROBLEM: ***"I am just starting a new business in a new city. How do I find out if I am in a high-crime area?"***

Discussion: Arrange for a security survey of any new location, particularly if you worry—or have some knowledge—that it may be in a high-crime area. That survey should include a comprehen-

sive summary of crime rates in your geographical area, so you can plan sufficient protection of your facility (see Part III-G, Working with the Police).

Resources:

- Local police department; and
- Security consultant.

PROBLEM: ***"I have had several thefts from one area of my warehouse, where eight employees are assigned. I want to polygraph them all!"***

Discussion: Recent changes in the polygraph laws severely limit your use of a polygraph in private industry. Do not offer (or threaten) a polygraph test without first obtaining competent legal advice (see Part III-F, Polygraph Examinations).

Resources:

- Corporate attorney;
- Labor law attorney; and
- Security consultant.

PART VI. SAMPLE FORMS AND POLICIES

MODEL SUBSTANCE ABUSE POLICY (*Maryland's Drug-Free Workplace Initiative: Keeping Maryland Business a Step Ahead*, Governor William Donald Schaefer's Advisory Board for Justice Assistance, December 1989).

DEFINITIONS AS USED IN THIS MODEL POLICY:

(a) "Substance" means alcohol or drugs.
(b) "Alcohol" means ethyl alcohol or ethanol.
(c) "Drugs" mean any substance taken into the body, other than alcohol, which may impair one's mental faculties and/or physical performance.
(d) "Abuse" means any use of any illegal drug, or any use of any drug, including alcohol, over the counter, or prescription drugs, where use is not in conformation with prescription requirements, or under circumstances where use is not permitted.

One of the greatest problems facing our society today is the abuse of drugs and alcohol. The nationwide impact of substance abuse in the workplace is now estimated to exceed $30 billion annually. This staggering amount only measures lost productivity and quality; it does not put a dollar value on personal pain and suffering.

The management of our company is vitally concerned about the well-being of our employees, our most valuable asset. We are equally concerned that our company's hard-earned reputation and positive image not be compromised in any way. Alcohol and drug abuse has an adverse effect on job performance, creates dangerous situations, and serves to undermine our customers' and the community's confidence in our company.

Our company cannot, and will not, condone drug or alcohol abuse on the part of our employees, nor will we condone any employee behavior on- or off-the-job that may serve to damage the company's reputation. Our policy concerning drug and alcohol use and abuse is as follows:

- Our company will not hire anyone who is currently known to abuse substances.
- Our company will educate and inform our employees about the health consequences of drug and alcohol abuse.
- Employees must report to work in a fit condition to perform their duties. Being under the influence of drugs or alcohol is not acceptable.
- Any employee on company business, on or off company premises, is prohibited from purchasing, transferring, using, or possessing illicit drugs or using alcohol or prescription drugs in any way that is illegal, or counter to published policy.
- Employees will not be terminated for voluntarily seeking assistance for a substance abuse problem; however, performance, attendance, or behavioral problems may result in disciplinary actions up to, and including, termination.
- Employees on physician-prescribed medication must notify a designated company official if there is a likelihood that such medication could affect job performance and safety.
- Employees arrested for off-the-job drug or alcohol involvement may be considered to be in violation of company substance abuse policy.
- Where available evidence warrants, our company will bring matters of illegal drug or alcohol use to the attention of appropriate law enforcement authorities.

PROGRAM OPTIONS

In order to implement a substance abuse program based upon the above model policy, your company must decide what program options it wants to offer. Suitable options--and the possible features they might contain--are included for consideration. To facilitate their review, the optional features are synopsized:

Prevention and Education

- Inform management of the nature, extent, and consequence of substance abuse within the work force and the prospective work force market, even if specific acts do not manifest themselves, thereby obtaining a commitment to work towards a drug-free workplace.
- Disseminate to all managers, employees, and prospective employees the company's written policy on substance abuse through the usual route of personnel communications.
- Provide employees, with the aid of employee groups if appropriate, accurate information on the legal, physical, and psychological consequences of on-the-job and off-the-job substance abuse.
- Train all supervisors and, where appropriate, representatives of employee groups, about drugs and paraphernalia; signs and symptoms of substance abuse; and performance deterioration signals, which aid them in implementing the company's substance abuse policy.
- Provide a list of public and private resources available to managers and employees that will assist them in addressing their substance abuse prevention, intervention, and treatment needs.

Enforcement and Performance

Drug Testing

1. Each employer should consider the value of pre-employment drug testing for all appropriate candidates. Obviously, such pre-employment testing must be within the boundaries of existing law, economically feasible for the employer, and based upon a careful analysis of the positions for which testing is required.
2. Each employer should consider the value of "for cause" drug testing, and testing that is provided within a treatment program. Employers should, when there are clear indications of performance problems that are related to drug use, require that individuals submit to an established testing protocol. Similarly, individuals enrolled in treatment programs may be required to submit to drug testing.
3. Employers should require random testing for all employees in appropriately designated sensitive positions.
4. Employers should require random testing during any routinely required physical examination.
5. Any drug testing must be carried out in compliance with carefully developed, comprehensive testing protocols that have been reviewed by, and disseminated to, all employees. The drug testing standards contained in the Mandatory Guidelines for Federal Drug Testing Programs are recommended.

Detecting Substance Abuse

1. All managers and supervisors should be trained to identify job performance problems that may be caused by substance abuse, and to be aware of the appropriate response to such problems.
2. Employers should consider establishing some method that would enable employees to confidentially or anonymously report any drug supplier in the workplace. The method must be used with full respect for the rights of all parties concerned. Information received through this method should be thoroughly and completely investigated before any action is taken by the employer.

PROGRAM OPTIONS (CONT'D.)

The Role of Law Enforcement Agencies

1. Employers should meet with appropriate local government agencies (e.g., law enforcement agency, office of alcohol and drug abuse coordination, etc.) to establish an agreement concerning the role each will play in responding to drug abuse in the workplace. Such an agreement usually should begin with an assessment of the situation. An effort should be made to determine the knowledge and understanding the employer, key managers, and line supervisors have regarding drugs in the workplace. If training is required, basic training may be provided to supervisors and managers.

2. In emergency situations, such as when sale or use of illegal drugs are observed, local law enforcement should be contacted using the appropriate emergency telephone number. The employer should, as with any emergency situation, be able to describe the activity observed, and identify involved persons and witnesses, etc.

3. If an employer suspects specific substance abuse acts are occurring within the workplace, but has no direct knowledge of such activity, local law enforcement should be contacted to discuss what kind of investigation is most appropriate.

4. Employers should understand that when assistance is requested from local law enforcement, and a criminal proceeding is subsequently initiated, they will be expected to support the criminal proceeding by testifying, providing paid release time for others to testify, etc.

Rehabilitation

1. Companies should consider implementing Employee Assistance Programs (EAPs) because these programs have a positive impact on people with problems, facilitate positive management/labor relations, encourage problem resolution, maintain an employee's dignity and confidentiality, and provide a return on the company's investment.

2. An EAP should be open to all employees on a self- or supervisory-referred basis for the purpose of information, advice, referral, or counseling. The purpose of counseling in the EAP is to assist employees with problems which impact adversely upon work performance or conduct. When these problems are effectively confronted and treated, the employees are expected to become healthier, better-adjusted individuals and are likely to perform more productively in their jobs.

3. Supervisors, other appropriate management, and union personnel should be trained in recognizing employees with problems and how to utilize the EAP.

4. Except for limitations on sensitive positions, no employee's job security or promotional opportunity should be jeopardized by a request for counseling or outside referral assistance from the EAP in connection with alcohol or drug abuse or emotional problems.

5. An EAP should operate under a clearly-defined policy which outlines the purpose of the EAP, organizational and legal mandates, employee eligibility, roles and responsibilities of various personnel in the organization, and procedures for program use.

6. A company should review its health benefits package for the purpose of determining adequacy of coverage for alcohol and drug abuse problems.

SAMPLE DRUG ABUSE POLICY STATEMENT

(Company Letterhead)

DRUG ABUSE POLICY STATEMENT

(Company Name) is committed to providing a safe work environment and to fostering the well-being and health of its employees. That commitment is jeopardized when any (Company Name) employee illegally uses drugs on the job, comes to work under the influence, or possesses, distributes, or sells drugs in the workplace. Therefore, (Company Name) has established the following policy:

(1) It is a violation of company policy for any employee to possess, sell, trade, or offer for sale illegal drugs or otherwise engage in the illegal use of drugs on-the-job.

(2) It is a violation of company policy for anyone to report to work under the influence of illegal drugs.

(3) It is a violation of company policy for anyone to use prescription drugs illegally. (However, nothing in this policy precludes the appropriate use of legally prescribed medication.)

(4) Violations of this policy are subject to disciplinary action up to and including termination.

It is the responsibility of the company's supervisors to counsel employees whenever they see changes in performance or behavior that suggest an employee has a drug problem. Although it is not the supervisor's job to diagnose personal problems, the supervisor should encourage such employees to seek help, and to advise them about available resources for getting help. Everyone shares responsibility for maintaining a safe work environment, and co-workers should encourage anyone who may have a drug problem to seek help.

The goal of this policy is to balance our respect for individuals with the need to maintain a safe, productive, and drug-free environment. The intent of this policy is to offer a helping hand to those who need it, while sending a clear message that the illegal use of drugs in incompatible with employment at (Company's Name).

NOTE: If your company is subject to the requirements of the *Drug-Free Workplace Act of 1988*—by nature of a grant/contract with the federal government—you should add the following statement to your drug policy:

As a condition of employment, employees must abide by the terms of this policy and must notify (Company Name) in writing of any conviction of a violation of a criminal drug statute occurring in the workplace no later than five calendar days after such conviction.

SAMPLE LETTER TO EMPLOYEES TO ACCOMPANY DRUG ABUSE POLICY STATEMENT

(Company Letterhead)

LETTER TO ALL EMPLOYEES

The illegal use of drugs is a national problem that seriously affects every American. Drug abuse not only affects individual users and their families, but it also presents new dangers for the workplace.

The President of the United States has urged business and labor to take a leadership role in a nationwide effort to reduce the illegal use of drugs.

As you are aware, (Company Name) has always been committed to providing a safe work environment and fostering the well-being and health of our employees. Illegal drug use jeopardizes this commitment, and undermines the capability of (Company Name) to produce quality products and services.

To address this problem, (Company Name) has developed a policy regarding the illegal use of drugs that we believe best serves the interests of all employees. Our policy formally and clearly states that the illegal use of drugs will not be tolerated. This policy was designed with two basic objectives in mind: (1) employees deserve a work environment that is free from the effects of drugs and the problems associated with their use; and (2) this company has a responsibility to maintain a healthy and safe workplace.

I believe it is important that we all work together to make (Company Name) a drug-free workplace and a safe, rewarding place to work.

Sincerely,

President
(Company Name)

MODEL SEXUAL HARASSMENT POLICY

(Company Name) does not tolerate sexual harassment in the workplace, or in a situation which is work-related. Sexual harassment includes:

(1) Unwelcome sexual advances;

(2) Requests for sexual favors and other verbal or physical conduct of a sexual nature when:

(a) submission to such conduct is made a term or condition of an individual's employment;

(b) submission to or rejection of such conduct is used as the basis for employment decisions affecting the individual;

(c) such conduct has the purpose or effect of unreasonably interfering with an individual's work performance, or creating an intimidating, hostile, or offensive working environment.

While it is not the purpose of this policy to regulate an employee's personal morality, (Company Name) considers sexual harassment to be an act of misconduct, and grounds for disciplinary action up to, and including, discharge.

If you believe that you (or another employee) have been a victim of sexual harassment, you should immediately report the matter to your supervisor or, if you wish, to a Company official. If an employee chooses to report the matter to his or her immediate supervisor, the supervisor must immediately report the matter to his or her department head, so that the complaint may be investigated promptly. An officer of the Company will be responsible for conducting the investigation. All complaints and information provided during an investigation will be kept strictly confidential. This policy prohibits any retaliatory action against any employee raising a complaint or providing information concerning ar alleged violation of this policy.

MODEL COMPUTER/DATA SECURITY POLICY

DEFINITIONS USED IN THIS MODEL POLICY

a. "Computer" means any electronic machine capable of accepting, processing, and/or manipulating alpha-numeric data according to programs and/or programming.

b. "Data" means any computer or electronically entered, generated, or retrieved information that may be reviewed on-line or copied on-line or via paper copies.

c. "Security" means the protection of computer and/or electronically-based information against unlawful or unauthorized disclosure, modification, or destruction.

Infringement upon computer/data security is a serious problem in our technological society today. Computer viruses are a reality, as witness the "Michelangelo" scare in 1992. Unauthorized or illegal access and modification to computers and their data and programs will not be sanctioned by (Company Name). All activity performed under any individual's User-ID/Password must be treated as highly sensitive information and must be restricted to the individual to whom the User-ID/Password is assigned.

THE BASIC FUNCTIONS OF (COMPANY NAME'S) COMPUTER/DATA SECURITY SYSTEM ARE TO:

- Allow authorized users specified degrees of access to protected information
- Prevent all access by unauthorized users
- Record all access to protected information for later reference
- Provide timely visibility of attempted computer/data security violations

COMPUTER/DATA SECURITY AT (COMPANY NAME) DEPENDS UPON:

- Commitment to computer/data security at all levels of management and staff
- Awareness and commitment to computer/data security by end-users
- Physical security of all computer components
- Implementation of the best available software/hardware security
- Intelligent computer/data security administration

(COMPANY NAME) WILL PROTECT ITS COMPUTER/DATA FUNCTIONS AS FOLLOWS:

I. Legitimate users will be required to:

A. Protect their user identification (User ID) and authentication information (such as a PIN, password, or token) and promptly report accidental disclosure or compromise to the appropriate custodian or systems administrator.
B. Access only files authorized.
C. Protect sensitive information from view by unauthorized persons.
D. Prevent unauthorized access to logged-on terminals or workstations.
E. Destroy printouts according to the procedure of destruction of documents as outlined in these procedures.
F. Lock or otherwise secure personal and portable computers, printers and other devices with buffers, when unattended, and remove and securely store removable magnetic and optical storage media, as well as printed output containing sensitive information.

MODEL COMPUTER/DATA SECURITY POLICY (CONT'D.)

G. Protect access to information on portable computers used outside (Company Name's) premises using security-approved facilities.

H. Comply with the security procedures specified by the custodian, systems administrator, and the corporate/divisional information management's procedures and standards.

I. Promptly report any unusual or suspicious occurrence to the custodian or the systems administrator.

II. Originators (of new files containing sensitive information, having first input on a specific subject to a data base, or first run on a particular system) shall also comply with the procedures for users (above), as well as the following:

A. Networked computers (e.g., mainframes, servers, and workstations)

1. (Company Name's) Confidential and Private Information

a. Classification notice:

- For new applications, display the classification notice at the top of the screen and provide that the notice appears wherever the data is displayed or printed.
- For existing applications, provide for proper classification display during program maintenance.

b. Provide the custodian or systems administrator with a list of users and/or job functions authorized to read, change, or delete information.

c. Contact the custodian or systems administrator to change user and/or job function access authority.

d. Inform the custodian or systems administrator and appropriate users when the information is no longer classified (Company Name) Confidential. Private information is not declassified; it is only deleted/erased.

2. (Company Name's) Restricted Information

a. Recognize that the computing system's highly privileged users, such as systems software maintainers, can access the information unless extraordinary measures are taken to avoid such a situation.

b. Contact the local information systems security coordinator regarding special security measures, including encryption

c. Provide the custodian or systems administrator with a list of users authorized to read, change, or delete information.

d. Classification notice

- Provide for the following notice to appear whenever the information is displayed to a requester. This notice shall display prior to the content of the requested information.

(COMPANY NAME) RESTRICTED CONTROL NO. _____

ONLY AUTHORIZED PERSONS ARE PERMITTED TO REVIEW THE FOLLOWING INFORMATION. UNAUTHORIZED PERSONS SHOULD IMMEDIATELY TERMINATE THIS REQUEST. IF YOU HAVE ANY QUESTIONS ABOUT YOUR AUTHORIZATION, CONTACT YOUR MANAGER.

MODEL COMPUTER/DATA SECURITY POLICY (CONT'D.)

- Provide for the classification and control number to appear at the top of the screen whenever the data is displayed or printed. (All copies shall be authorized and accounted for by copy number.)

e. Establish an accountability record, and include the control number, as specified by the originator. When printing a copy, a sequential copy number shall also be displayed to the right of the control number.

f. Contact the custodian or systems administrator to change user access authority and to request erasure of data.

g. Inform the custodian or systems administrator when the information is reclassified as (Company Name) Confidential, or is no longer classified.

B. Personal Computers (and other stand-along computers not on a network)

1. Display the appropriate classification and notice (and copy number, if (Company Name) Restricted) on all printed output, as well as electronically stored images.

2. Promptly erase (or otherwise render useless) electronic media containing sensitive data no longer required. Simple functions such as "delete" or "erase" do not destroy the data; they simply remove the pointer to the data. More thorough measures, such as those described in below, may be required.

III. Custodians (those responsible for the maintenance and distribution of an information resource) shall also comply with the procedures for users, as well as the following:

A. Assure that the classification notice designated by the originator is displayed as required by those procedures.

B. Assure that each program and/or file presents only information consistent with the requester's authorization.

C. Protect documents or files containing passwords or other identity authentication information in the same manner as with (Company Name) Restricted information.

IV. Systems Administrators

A. Obtain access authorization for each file (read, change, delete, execute, etc.)

B. Manage user identification and authentication facilities, such as password systems, consistently with (Company Name's) computer/data and telecommunications security and control standards.

C. Promptly implement changes in access control systems when users' access authorities change, including their move from one assignment to another, as well as when they leave (Company Name).

D. Consistent with records retention guides, erase data when the information is no longer required by the originator, his/her successor, and users. Prior to erasing (Company Name) Restricted data, contact the originator for approval and appropriate notation on the accountability record.

1. Files: Overwrite disk files and verify the obliteration or erasure of the data. Overwrite files containing (Company Name) Restricted information even though they may be encrypted.

MODEL COMPUTER/DATA SECURITY POLICY (CONT'D.)

2. Removal media (disks, diskettes, cassettes, cartridges, etc.): Demagnetize and verify erasure prior to reuse, transfer to others, or destroying.
3. Fixed or hard disks: Clear through initialization, reformatting, overwriting, or similar means, and verify erasure before transfer to others (including repair services) or destroying.

E. Report suspicious occurrences, such as unexplained failed log-on or information access attempts, to management and to (Company Name) security.

(COMPANY NAME) WILL PROTECT AGAINST UNAUTHORIZED VERBAL DISCLOSURE AS FOLLOWS:

I. Who

A. Discuss (Company Name) Confidential information only with employees, subcontractors, suppliers, etc., who have a "need to know." If in doubt, contact the appropriate manager or originator of the information.

B. Discuss (Company Name) Restricted information only with those individuals approved by the originator.

C. Discuss (Company Name) Private information only with those directly concerned.

II. Where

A. At (Company Name) facilities, conduct discussions, meetings, and conferences involving highly sensitive subjects only in areas:

1. Where access can be controlled
2. That provide sound insulation
3. That have been carefully examined to locate any device that could record or transmit the proceedings. If such devices are present, make them incapable of recording or transmitting the proceedings, unless the recording or transmission has been authorized by management.

MODEL COMPUTER/DATA SECURITY CHECKLIST:
EVALUATING YOUR COMPANY'S POLICIES AND PROCEDURES REGARDING CONFIDENTIAL (PROPRIETARY) INFORMATION

GENERAL

- Is management aware of the need for protecting confidential information?
- Who is responsible for protecting confidential information?
- What types of confidential information are kept at your facility?
- Are employees who handle confidential information briefed as to their responsibility to discuss it only with those having a "need to know"?

DOCUMENTS

NOTE: Examples of confidential information are: advertising strategies, marketing plans, trade secrets, stocks, bonds, and trading information, client lists, customer information, price lists, labor negotiations, political strategies, hiring and firing information, employee personnel records, court cases, trial preparation client lists, and any other information that can give one entity and advantage over another.

- Are sensitive documents secured when not in use?
- Are sensitive documents controlled on a need-to-know basis?
- Are your Company Confidential and Company Restricted markings utilized?
- Are safeguards identified and followed for paper waste, collection, and destruction?
- Who instructs your employees in the control and handling of sensitive information?
- Are desk and cabinet tops cleared at the end of the day?
- Are file cabinets locked at night and on weekends?
- Are safes used?
- Do you utilize shredders?

COMPUTERS/DATA PROCESSORS

- Are personal computers housed in locking workstations? How are lap top computers secured? Where are keys kept?
- Do files have password protection?
- Are diskettes kept in locked diskette cases or a locked cabinet?
- Are disk power supply locks utilized?
- Are backups make of all important information? How often?
- Are keys to personal computer diskette cases, desk drawers, and cabinets available from a controlled source, e.g., secretary, security?
- Are all base components (including printers, personal computers, plotters, monitors, etc.) logged by asset tag number or serial number?

CUSTODIAL SERVICE

- Is your service in-house or contractual?
- What hours does the service start and complete work, and how is that monitored?
- Does the service possess keys to your facility? If so, how do you control those keys?
- Are there controls for custodial access to office space? manufacturing areas? storage/warehouse facilities?
- Are police records checked for custodial employees?

CLASSIFIED TRASH

- Is a "classified trash" pickup service utilized?
- What is the frequency of pickup?
- Is the location or method of destruction (burn, shred, compact) subject to interference?
- Has your company security personally inspected the destruction method and site?

Acknowledgements

We wish to acknowledge and say "thank you" to the following people and organizations for their assistance and encouragement. Without them, this project would not have been as enjoyable or successful.

Rebecca P. Gowen, Administrative Officer of the Maryland Parole Commission, for her unselfish work in helping us edit and link the "loose threads" of this publication.

William L. Cotton (Assistant Task Force Chairman), of Cotton-Hyson Protective Services, Inc., for his unfailing assistance throughout the course of this project.

Philip H. Cogan, formerly Senior Policy Analyst of the Office of National Drug Control Policy, Executive Office of the President, for his hard work and support in making this a better publication.

Mary K. Dueppen, President of Paw Print Publishing, who spent countless hours shaping the final product.

The following individuals met with the task force and provided us their expertise and knowledge:

Gale R. Caplan, Chief
Medicaid Fraud Control Unit
Maryland Attorney General's Office

John Drenocky, Manager
Special Investigation Division
United States Fidelity and Guaranty

Anthony R. Gallagher
Office of the Federal Public Defender

Howard Glashoff, Security Chief
Baltimore City Dept. of Public Works

Haven Kodeck, Chief
Economic Crimes Unit
Baltimore City State's Attorney's Office

Thomas Levering, Captain
Baltimore County Police Dept.

John F. Lewis, Special Agent
United States Secret Service
Washington, D.C.

The following individuals reviewed the documents at various stages of completion and provided their valuable insight:

Pam Collins, Ph.D., Security and Loss Prevention Program, Eastern Kentucky University

William Highfield, Board Member, International Association of Crime Prevention; Officer, Westerville, Ohio, Police Dept.

Mary Ann Saar, Secretary, Maryland Dept. of Juvenile Services

The following members of the task force attended numerous meetings over an 18-month period and generously assisted us in the writing of this publication:

James R. Crook, Chief of Legislation (Ret.)
Baltimore City Solicitor's Office

Joseph K. Deegan, Agent (Ret.)
Federal Bureau of Investigation

Michael F. DiMaggio
Federal Armored Express

Drake Ferguson, CEO
Foxfire Network Services

Jerome L. Frank, Account Executive
Medex Corporation

Richard Govignon, Security Consultant
Card Key Systems

Theodore S. Moyer, Major (Ret.)
Maryland State Police
Former Harford County Sheriff

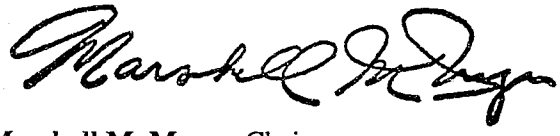
James L. Scannell, Captain (Ret.)
Baltimore County Police Dept.

Patricia L. Sill, Administrator
Maryland Community Crime Prevention Institute

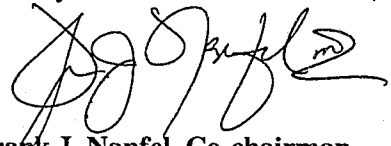
Harvey M. Soldan, President
Diversified Real Estate and Business Enterprises

James W. Yeasted, Captain
Baltimore County Police Dept.

This publication would not have been possible without the input of all of these people who gave unselfishly of their time and effort.



Marshall M. Meyer, Chairman
Governor's Executive Advisory Council
Security Consultant and President, MSA, Inc.



Frank J. Napfel, Co-chairman
Impact of Crime on Business in Maryland Task Force
President, Baltimore Security Systems, Inc.

Kai R. Martensen, Co-chairman
Impact of Crime on Business in Maryland Task Force
Principal Associate, Institute for Law and Justice