CRIME IN SERVICE INDUSTRIES

U.S. DEPARTMENT OF COMMERCE
Domestic and International
Business Administration

43506

CRIME IN SERVICE INDUSTRIES

U.S. DEPARTMENT OF COMMERCE
Domestic and International Business Administration
September 1977

FOREWORD

Crime cost American business an estimated $30 billion in 1976. Losses have exceeded $9 billion in the service sector alone. These data are 11 percent higher than comparable 1975 data outlined in the February 1977 revision of The Cost of Crime Against Business.

Although many of the reasons behind the continually rising losses remain unclear, the implication of the steady rise in crime is very clear: management involvement in the battle to cut losses is not sufficiently aggressive. Management has responsibilities not only to recognize crime as an unnecessarily high expense, but also to recognize steps it can take to reduce this expense and to take the initiative in implementing cost-cutting policies.

This publication provides guidelines for crime deterrent policy formulation in the service sector, and identifies primary vulnerabilities of service businesses to crime. It is directed toward the management level, and emphasizes the executive role toward achieving reduced losses.

Although the product of this sector of the economy is intangible, the service process requires a concentration of labor and an infinite variety of consumer goods. Consumer products are targets for theft because of their high resale and personal use value. These are the assets that, when stolen, drain profits and lessen competitive status. The labor intensity of the industries further exposes the assets to risks. Combined with the possibility of damage to public relations caused by vulnerability to consumer victimization, service business crime poses a severe problem demanding assertive management attention.

Computer abuse imposes additional losses upon the service sector, as it does upon all industry. Losses by computer crime are rising and it is clear that management reluctance to establish authority over computer operations heightens vulnerability. This crime, long considered a crime of the future, has become reality and is keeping pace with increasing sophistication of technology.

The controls most likely to counter the impact of crime in the service sector are employee oriented. Comprehensive pre-employment screening, training, and participatory management are imperative, not only to insure the integrity of the staff, but to build a staff capable and willing to protect assets from external threats, which are many and unpredictable in the service sector.

The information contained in this report was developed through intensive research and in cooperation with Federal and State government and industry sources. Suggestions on loss control were developed with the assistance of industry experts. Valuable insight to service industry crime problems has been gained through a series of seminars on crimes against business conducted by the Consumer Goods and Services Division, Office of Business Research and Analysis in the Bureau of Domestic Commerce. The constructive exchange of ideas among government, industry and security representatives will continue to impart a clearer perspective of the issues, obstacles, and opportunities facing industry in .ts effort to reduce crime losses.

The report was developed by Sharon Roach assisted by Beatrice DeLoatch, under the direction of Mr. Thomas E. Murphy, Acting Director, Consumer Goods and Services Division.

CHARLEY M. DENTON
Director
Office of Business Research and Analysis

STANLEY J. MARCUSS
Deputy Assistant Secretary for
Domestic Commerce

TABLE OF CONTENTS

INTRODUCTION

This report discusses the impact of crime on the services sector. The third in a series of Department of Commerce reports on the cost of crimes against business, the report provides, in Section I, an overview of the problem as well as chapters on individual services. Financial, educational, cargo transportation, hospitals, lodging, property and casualty insurance and certain miscellaneous services for which information was obtainable are included. Specific vulnerabilities, losses and applicable deterrent measures are identified to the extent possible, and case studies have been included to illustrate key security principles. Section II addresses specific crimes and suggests guidelines for management policies to reduce losses stemming from these crimes. Computer crime, employee theft, and bad checks are discussed. Also in Section II, specific attention is directed toward the policy of pre-employment screening as a fundamental deterrent to employee theft. To complete that discussion, the impact of privacy, civil rights and credit legislation upon pre-employment screening is examined.

Individual service industries were selected for inclusion as chapters on the basis of the type of crime experienced, geographical diversity, data availability, and cooperation of industry executives and trade associations. Industries were selected from which effective principles of crime loss reduction could be derived and applied to other industries not specifically addressed in individual chapters.

The specific industries covered in this report are at uneven stages in developing industry-wide crime loss reduction policies. Most services have only recently begun to assess the impact of crime upon their particular industry; as a result, many alternatives in crime loss prevention are just emerging. Some services, such as transportation and banking have reacted rapidly to the problem, prompted by federal regulatory requirements. Others, such as health care and lodging have made much slower progress in achieving industry-wide results.

The vulnerabilities to crime existing in these services are diverse. Employee theft is more prevalent than other crime, while losses in the property and casualty insurance services stem primarily from swindlers -- with only infrequent internal/external collusion, and educational losses stem from vandalism and theft.

Case examples illustrate effective approaches to crime control, and the principles found in these approaches are relevant to any security program in any business, whether goods or service producing.

Taken together, Section I and II provide concrete guidelines for aggressive management action to reduce the impacts of both the crime and the loss on the services sector.

Any questions concerning the report should be directed to Sharon Roach, Room 1104, U.S. Department of Commerce, Washington, D.C. 20230. (202-377-4697).

SECTION I
OVERVIEW

The Economic Impact of Crime in the Service Industries

The service sector accounts for almost two-thirds of U.S. economic output and consumption. Two-thirds of the American labor force are service employees.

Services are distinct from other economic sectors in that they produce intangible output. Each service is unique -- with different production processes, customers, suppliers, and marketing methods. Thus, this sector is basically a grouping of distinct industries -- categorized together only because the output is service, rather than tangible products.

An analysis of crime in this sector reflects the heterogeneity of the services: generalization is difficult. Unlike retailing, manufacturing or wholesaling, crime problems in any given service are extraordinarily diverse with far more significant ramifications. The economic impact of the loss on the business often is compounded by the psychological impact of the crime on the consumer, which ultimately decreases profits or decreases the ability of the business to render quality service.

Losses

Based on research conducted for this study, crime costs the services sector at least $9.2 billion annually. Table I highlights losses of selected services.

Compiled by the Bureau of Domestic Commerce, the cost data include estimates based on industry consultation. The inclusion of estimates in Table I causes the figures to vary with those in the text. While the text figures represent partial statistical reporting by industries, in most instances, the estimate in Table I should be considered as a guideline and not as an inflexible measurement.

TABLE I

Estimated Cost of Crime in Selected Service Industries[1]

Sector	Dollar Cost in Billions[2]	
Cargo Transportation	2.5	
Air		.4
Rail		.6
Truck		1.2
Maritime		.3
Passenger Transportation (Air)	.1	
Education	.7	
Financial Depository Institutions	1.7	
Health Care Services	1.0	
Lodging	1.5	
Property, Casualty Insurance	1.5	
Miscellaneous	.2	
Total	9.2	

[1] Source: Bureau of Domestic Commerce

[2] These cost data include estimates, based on industry consultation

This estimate -- $9.2 billion -- understates the cost of crime in the services, although by how much is unclear. Preventive costs such as insurance premiums, security programs and prosecution expenses are excluded. These costs defy aggregation in any meaningful sense for the sector. Subsidiary costs of crime in this sector such as loss of reputation and deterioration in the quality of service rendered cannot be computed in a quantitative sense, and thus are not included. It is important to realize, however, that these are costs of crime to this sector.

Moreover, many services experience crime problems that are necessarily beyond the scope of this report. Corruption -- bribery, kickbacks, fraud -- is present in many services, as it is in most business. Frauds against consumers, and professional fraud -- such as bankruptcy fraud -- are also business crimes. To assess the economic and social impact of these crimes is not feasible and has not been attempted in this report.

Most important, the figure cannot be adjusted for unreported crime, which is substantial in the services sector as it is in all business. For some entire industries, there is a complete lack of figures. Although the phrase has become over-quoted, known crime in the services sector is merely the "tip of the iceberg."

Crime Problems in Perspective

The impact of crime on this sector is not diminished by the absence of a comprehensive statistical estimate of its cost. Rather, the lack of such data is only one of many problems facing the service sector in its generally formative stage of dealing with the crime issue. Distinct similarities in crime problems exist among the services industries:

The lack of comprehensive data is common to all. Some industries are required by law to report losses to Federal agencies, thereby providing partial insight into crime impact. Other industries, through trade associations, have undertaken membership surveys that provide partial insight. These partial insights are a beginning, and need to be developed more extensively.

Many alternatives to crime loss prevention are just emerging, because most services have begun only recently to assess the impact of crime upon their particular industry. Approaches tend to be fragmentary because of the relative newness of the problem. The escalation in public concern over law and order, as well as intensified economic pressures in recent years, have imparted urgency to the effort to reduce crime and losses, with the result that planning is often haphazard.

Employee theft is a primary cause of crime losses in the services, although external threats such as burglary, robbery, larceny, bad checks and fraudulent use of credit cards are also present. There are industries to which this does not apply in a traditional sense -- education and certain other professional services, but it does apply to the majority of customer oriented, profit producing establishments. Employee theft results from the nature of inventories stocked, the intensity and composition of the labor force, and the lack of managerial controls designed to create an honest, reliable work force.

Computer abuse is a potentially devastating crime to the services, some of which are the most automated in all industry. Financial and insurance sectors are more exposed to the risk of loss through computer abuse due to the totality of reliance upon automation, although it must be emphasized that an improperly protected computer in any business is vulnerable to compromise or sabotage.

The availability of similar security measures is an additional factor common to all services. An effective program to reduce crime losses contains three elements in some form: employee control, based on participative management; comprehensive auditing; and a philosophy of deterrence that anticipates the crime. An effective security program does not mean the elimination of crime losses, as even the most stringent efforts will not enable a firm to avoid crime. An effective security program, rather, must be one that reduces losses to a minimum. At the same time, an effective security program leads to improved profits. An organization simply can't afford not to initiate comprehensive policies from the managerial level.

The often contrasting concepts of security and services -- consumer accommodation -- is the fundamental problem most services face when attempting to reduce losses. A successful service is closely allied with consumers and a crime deterrent program, if not carefully structured, can disrupt the alliance if consumers feel harassed. The conceptual conflict between security and service is an obstacle to maximum loss reduction for many services. The danger always exists that consumers may complain of arbitrary and unnecessary harassment because of a company's adherence to a security program. But, as in any business, consumers must be educated to the need for security measures and must understand that it is to the consumers and management's ultimate benefit -- i.e., lower prices through cost reductions -- that prevention programs be implemented.

Determination of Crime Vulnerabilities in Service Sector

Crime vulnerabilities in service industries not identified in the following chapters depend primarily on the characteristics of the individual industry. More specifically, the potential severity of the two main sources of losses -- internal and external -- is a function of the interrelationships among the industry's consumers, employees, and the actual process of service production.

Professional services such as legal, advertising, medical and funeral, for example, are exposed to complex risks of loss from internal theft -- primarily fraud and embezzlement. These white collar crimes tend to be larger in scale, although less in frequency, than internal theft in the form of pilferage. Risks to crime losses perpetrated by consumers -- bad checks, credit card losses, fraudulent claims and associated activities -- are minimized through the mechanics of the service production process and consumer - service relationship.

To reduce vulnerabilities from internal losses, management of professional services must establish a stringent program of accountability and comprehensive auditing -- similar to programs that effectively control risks in financial services.

Other services, particularly such labor saving services as restaurants and fast food franchises, employ completely different processes of producing services. Internal theft -- pilferage -- is a major loss area in restuarants, for example. More specifically, employee theft of food is a potentially critical loss area, based on the access employees have to food, and food's high resale and personal use value on the outside.

Restaurants are also more frequently exposed to armed robbery, burglary and embezzlement of cash. Moreover, because employees use cash registers, businesses are vulnerable to employee pilferage of cash, through under-rings and shortages.

Effective preventive measures in these services parallel those applicable to services such as lodging or hospitals. Accountability of inventory is imperative, and if turnover prevents implementation of an effective personnel policy, losses can be controlled through restricting exits, package inspection, separation of employee parking from the main building, closer supervision and other standard dishonesty controls discussed in individual chapters and in Section II.

Services that depend to a significant degree on consumer payment by check and credit cards -- which include a broad spectrum of personal services and labor saving services -- face additional losses if basic controls are not established.

Beyond the insight to crime that can be gained from industry-wide characteristics, there are a host of basic factors that influence crime frequency and incidence in individual companies in individual communities. For example, the Federal Bureau of Investigation specifies the following factors as affecting the volume and type of crime occuring in the nation:

- Density and size of the community population and the metropolitan area of which it is a part.
- Composition of the population with reference particularly to age, sex, and race.
- Economic status and modes of the population.
- Stability of population, including commuters, seasonal, and other transient types.
- Effective strength of the police force.
- Policies of the prosecuting officials.
- Attitudes and policies of the courts and corrections.
- Relationships and attitudes of law enforcement and the community.
- Administrative and investigative efficiency of law enforcement, including degree of adherence to crime reporting standards.

The impact of crime in the services sector compares to the impact of crime on other sectors. The problems are essentially the same: sparse data, low level of awareness, similar vulnerabilities, and designing security to minimize the losses.

The task services face is parallel to other sectors, as well -- resolve these problems as urgently and efficiently as possible in the face of escalating economic and social pressures to lessen the impact of crime on business.

The following chapters and loss reduction policy suggestions offer insight into alternative resolutions.

Chapter 1

CARGO TRANSPORTATION

Cargo transportation services are unique among industries examined in this report in that crime problems have been the subject of in-depth study by both the industry and Government.

Executive Order 11836 signed by the President in January 1975, emphasized the need for "increasing the effectiveness of the transportation cargo security program" and stated that "theft of cargo has emerged during this decade as a serious threat to the reliability, efficiency and integrity of the Nation's commerce."

Generated at least partly by hearings conducted by the Senate Select Committee on Small Business in 1968-1972, concerning the impact of crime on small business, which focused on the lack of relevant data and lack of cause and solution analysis, both industry and Government are developing improved security programs.

More complete data, more concise definitions and more perceptive solutions concerning crime thus characterize the sector -- comprised of rail, truck, maritime and air, as well as a new form, pipeline.

The Executive Order formalized much of what, since 1972, had been purely voluntary efforts to remedy the deficiencies noted in the Senate hearings, and to reduce crime losses in recognition of the erosion of industry profits and inflation of consumer prices that these losses cause.

The Federal Government's concern with transportation crime, which is estimated at $2.5 billion in 1976, is spearheaded by the Department of Transportation, Department of Treasury (Bureau of Customs), and the Department of Justice. The National Cargo Security Program emphasizes voluntary industry cooperation; no mandatory controls have been imposed. In a March 31, 1976, report to the President, the Secretary of Transportation stressed that corporate enforcement of cargo accountability and the use of simple, basic security measures will prevent the largest proportion of theft losses. Prevention has been the key concept permeating the program.

The official federal forum on cargo security is the Interagency Committee on Transportation Security. Although Executive Order 11836 somewhat reduced its activities, this fourteen member interagency body is useful as a coordinating vehicle.

The private sector established an inter-industry committee, the National Cargo Security Council, sponsored by the Transportation Association of America. Each mode, moreover, has its own cargo security council.

The overall effect of these industry/government efforts has been positive. As will be seen, air cargo carriers have made the greatest progress, while the trucking sector has begun to show gradual improvement in reducing losses. There is still insufficient data by which to judge maritime losses, and rail transport losses are on the rise.

Trucking Cargo

The 23 1/3 million trucks that are registered in the United States are divided into two categories: private and for-hire carriers. Interstate Commerce Commission (ICC) regulated carriers transport at least one-third of all manufactured goods tonnage in the United States. Private carriers, shippers, manufacturers, or merchants using their own vehicles, transport another 35 percent of total, with the remainder by other modes.

The trucking industry's experiences with crime mirror those of the other modes, in that losses were high, at $1.5 billion, and security precautions rare, until the aftermath of the 1968-1972 Senate Select Committee hearings. The trucking industry, as other modes, was not fully cognizant of the extent of the problem.

A partial response to the situation was the formation of the Trucking Industry Committee on Theft and Hijacking (TICOTH), an operating unit of the American Trucking Association, Inc, (ATA), which was composed of motor carrier top management personnel.

A more comprehensive response was made in June 1976 with the creation of the ATA Security Council to complement TICOTH. Composed of motor carrier middle management security personnel, the Security Council's objectives are the development and maintenance of technical security programs needed for a more effective industry-wide program. According to industry sources, TICOTH's effectiveness had been diminished because of a lack of time and expertise.

Examples of initiatives the ATA Security Council have taken include development of a cargo security film and slide presentations designed to educate all segments of the industry to the advantages of a good cargo security program and to discuss effective security measures that can be implemented by motor carriers.

Losses

The table that follows summarizes loss and damage claims paid in 1975 due to shortage, thefts and pilferage, and hijacking, for certain key commodities. These data are representative of 10 percent, by revenue, of cargo carrying by trucking, and are based on quarterly reports filed with the ICC.

Theft-related claims paid in 1975 decreased 18.6 percent from 1974, and represent approximately 50 percent of all claims paid. Over 85 percent of theft-related claims are paid for shortage; 15 percent for hijacking, grand larceny, and burglary.

TABLE II

1975 Loss and Damage Claims Paid by Commodity, Number, and Value[1]

COMMODITY	SHORTAGE		THEFT & PILFERAGE		HIJACKING	
	Number	Value	Number	Value	Number	Value
Food[2]	52895	3052771	780	142995	19	240167
Clothing, Except Furs	56067	8349352	6134	2029794	90	16923
Cigarettes	1358	234855	198	320253	13	72592
TV's, Radios, Recorders, Amplifers Parts	15794	2686872	1972	1003905	33	324481
Auto, Bus, Truck Parts and Accessories	29374	2702081	334	104300	4	286
Drugs, Medicines	20664	973358	184	45457	3	299
Electrical Machine Equipment	16036	1869858	387	134210	12	1102
Metal Products	25363	2727559	269	79463	140	530924
Hardwares, Except Power Tools	30426	2445733	1078	120996	7	525
SUBTOTAL	247977	25042439	11536	3981373	321	1187299
TOTALS [3]	732492	64301307	24942	6825119	448	1243941

[1] Source: Quarterly Reports, Loss and Damage Claims Paid; Value in dollars.

[2] Includes (1) canned, dried, preserved, pickled; (2) frozen fruits, vegetables and prepared meals; and (3) food or allied products, not otherwise included. Note: Hijackings were all in category (1).

[3] Includes all categories not listed in this partial table.

Added to the amount of claim payments are the administrative costs of processing claims and locating missing freight to avoid claim payments.

A 1975 study of truck crime in New York City conducted by the Security Council of New York State Motor Truck Association found that non-regulated carriers are the primary targets of crime. This survey reported that non-regulated carriers experienced over 80 percent of total reported thefts and over 70 percent of total monetary loss.

There is no feasible method by which to reevaluate these data to assess the impact on the 90 percent, by revenue, of cargo carriers that aren't represented in the above table. It is clear, however, that this $65 million understates the extent of losses to a significant degree.

Table II also identifies key commodities that are vulnerable to theft. Those listed are among 64 categorized on loss and damage claims paid reports. The common factors among these commodities are (1) their high resale value and (2) the ease of absorption into the market -- they are difficult to identify as being stolen goods. These factors are essential to the fencing process -- the distribution channel through which the majority of stolen goods are disposed.

An analysis of the bulk of items stolen in one incident, although not reflected in the above data, adds credence to the widely held theory that the fencing "industry" flourishes. For example, data extracted from small scale surveys of truck thefts conducted by a private alarm company indicates that the value of a single theft of cigarettes often exceeds $30,000 -- and in one 1974 incident, $250,000 worth of cigarettes were stolen from one shipment. In other single incidents, color TV sets, valued at $100,000; $260,000 of auto air compressors; $250,000 of camera equipment; and appliances worth a value of $500,000 were stolen.

The ready availability of illicit outlets for these goods serves to perpetuate the process of cargo theft-fence-legitimate markets. As is pointed out in other Department of Commerce publications such as the Cost of Crimes Against Business, merchants should take the initiative to close the access "fences" currently have to the legitimate market. This they can do by refusing to accept goods from unknown shippers or suppliers, for example.

Vulnerabilities

As is evident from the above figures, hijacking is the source of only a small percentage of theft-related claims. And, although greater opportunities for crime occur in or at the terminal, theft of shipments in transit -- hijacking -- has received a relatively greater degree of attention as to alternatives for loss reduction.

The vulnerability to hijacking which a trucking company faces is measured by environment, including geographical location, organized crime activity and the volume and type of business. The pattern of hijackings is easily regionalized: the Northeast United States, particularly the cities of New York and Boston, have higher rates, as do Chicago and Miami. This is due in part to the general crime rates in these locations, and their status as major trucking centers, which generates a high volume of business.

Hijacking is a one time event that usually causes high losses to the victimized company. One survey indicates that the average loss in cargo theft from trucks in route was $32,000 in 1975. Nevertheless, hijackings represent only 1 percent of claims in the industry.

Media coverage of hijacking resulted in a concerted effort by industry toward protecting both the cargo and the carrier through identification techniques. Truck top marking is one example; the system was initiated because such marking increases the ease and time within which a hijacked or stolen vehicle can be located by law enforcement helicopter patrols. An experimental program conducted by the Department of Transportation in 1972-1973 indicated that the markings were effective and relatively inexpensive. Costs for a group of 12 trucks ranged from $500 to $1,440, although costs would be reduced to as little as $30 per truck if the markings were done on a large scale -- at least 100, at a time, for example.

Another example of merchandise identification is electronic tagging. Although the Department of Transportation experiments have determined the technical feasibility of this method -- which enables location of vehicles or containers if hidden -- the amount of tagging time involved, coupled with the quantity of merchandise, makes the process unfeasible.

One factor that increases the difficulty in countering hijacking is collusion, or even blackmail, between the trucker and hijacker. There is no foolproof preventive measure that anticipates collusion, although an aggressive policy of employee controls can be effective, as is discussed in further detail, below.

Despite the emphasis on hijacking, the crimes that cause far greater losses, in the aggregate, are the "nickel and dime" thefts and pilferages. Internal and external pilferage is the theft of one or two cartons at a time, repeated on a continuing basis, the effect being a continual invisible drain. The extent of these losses is not reflected in the ICC data, partly because of the limitation in the scope of the industry affected by the reporting requirements, and partly because reporting is required only if losses exceed $100.

85 percent of these thefts and pilferages are traceable to persons authorized to handle freight, according to a Department of Transportation report.

While a significant percentage of cargo theft can be attributed to dockworkers and other facility workers, a comparable portion can be traced to drivers alone, or drivers in collusion with dockworkers. For example, a dockworker will deliberately overload the truck, and the driver will remove the excess freight enroute. The driver will have the correct number of pieces of freight to unload at the destination. This type of theft can be detected only at the loading dock, and if proper managerial controls are not in force, the theft probably won't be detected. There also have been instances of drivers "selling" their loads to thieves or fences, and then reporting the truck as stolen or hijacked.

Prevention of Cargo Theft

The trucking industry relies heavily on physical plant security, reflecting the increased vulnerability of cargo merchandise to theft and pilferage by employees and outsiders, if the premises are inadequately protected.

The extent and emphasis of plant security varies between companies and locations; no one standard of security will be cost-effective for all companies. Most trucking firms rely on at least one of the following components to an effective security system: lighting, fences, or security guards. Combinations are used when circumstances warrant. These security measures are in addition to alarm systems and locks -- basic to any security system.

Yard lighting is a basic, and industry sources indicate that it is, or should be, employed by most trucking companies. It is relatively inexpensive and highly valuable as both a deterrent to amateurs and an aid to security personnel faced with detecting intruders.

The cost of adequate fencing on the other hand, can be prohibitive -- especially to the company whose risks do not warrant the outlay. Fencing is most effective in populated areas, especially those areas with high crime rates, as its primary purpose is to prevent the non-professional burglar from gaining entry to the warehouse.

There are indications that companies who do erect fencing either fail to maintain it properly or fail to install it with security in mind. For example, the effectiveness of fencing is diminished if it does not extend all the way to the ground; leaving a space for persons to crawl under negates much of its deterrent value. Fencing that does not extend all the way to the ground still deters the larger, heavier cartons that can't be pushed under or thrown over. The effectiveness of fencing can be further reduced by too many gates which are potential sources of easy access. Fencing, furthermore, should be illuminated to aid the security officer in detecting the intruder, and to act as a deterrent to the would-be intruder.

The Department of Transportation's "Guidelines for the Physical Security of Cargo" sets forth applicable specifics on both lighting and fencing for the use of the industry.

The third standard component in security systems maintained by trucking companies are security forces, although companies with sufficient resources have found electronic surveillance devices to be an excellent substitute for, or supplement to, security forces. This is particularly true for operations with large facilities and many points of access.

While it is obvious that security forces -- the traditional visual deterrent -- situated at entrances and exits will deter some employee theft, additional use of the measure, by expanding the officer's function can benefit a security program. For example, a security officer should be able to perform limited searches of employee cars leaving the premises, for stolen merchandise. One firm established a policy whereby employees expect to be searched and are required to open their car trunks for easier inspection. The guard at the gate closes the trunk after inspection. Often, a brief visual inspection suffices; the employee is not delayed and thus does not feel harassed. Significantly, employees willingly participate in this policy.

Security officers can also be essential in the monitoring of ingoing and outgoing shipments. The extent of control which this element of security has over terminal operations is a management decision. Controls should be sufficiently strict at the point of loading and unloading that security at the gate is only a supplemental precaution.

Casual burglary losses are, to a large extent, deterrable through physical security measures. Additional measures enhance the basic precautions and entail little, if any, expenditure. Most important of these is maintenance of all physical security in proper working condition. Security personnel should be detailed daily to the task of checking installed security. This includes all devices, including locks and lights.

An example of innovative deterrence is parking loaded vehicles back to back in the terminal area. This increases the difficulty of removing the cargo by requiring the thief to move at least one of the trailers before gaining access to the other. This arrangement, by lengthening the time required for the theft, can act as a deterrent by increasing the risks.

A factor enhancing the seriousness of external theft other than casual burglary is its connection to internal dishonesty. Collusion between drivers and dockworkers undercuts physical security. This collusion, and the belief that a majority of losses are attributable to employee theft, make it necessary that internal policies be developed to deter employee dishonesty.

Employee theft controls are based on assertive management policies. A primary finding of a Department of Transportation study on security practices in cargo terminals is that management attention and good operating procedures are more effective in reducing losses than are complex security systems. In this respect, the trucking industry is similar to all industry in that effective security measures are in large part a function of management innovation and foresight.

Accountability should be the keystone of management policy with respect to security. Audit trails must begin at the point of first contact with the cargo and end only at the point of last contact. Supervisory presence is mandatory at loading facilities, and the cargo should be transported within a sealed container to discourage amateur thieves and allow for detection of theft. Seals are useless if controls over them are ineffective. Unissued seals should be protected in a locked container. Any discrepancies in numbers on the seal and shipping documents upon delivery should alert the responsible person to the necessity for an item-by-item inventory, for example. The Department of Transportation publication "Guidelines for Physical Security for Cargo," should be consulted for details in this regard.

Within the terminal, movement of high value merchandise should be containerized, whether or not it is being shipped immediately. This reduces the opportunities employees have to steal.

In addition to supervisory control and reduction of high value cargo expenses, easily implemented measures are available to further reduce employee opportunity to steal. For example, employee parking should be located away from the terminal area. Ideally, the facility should be a separately fenced area with only one exit monitored by qualified security. If this isn't feasible, parking must be removed from cargo areas; otherwise the temptation to steal and the ease of theft is overwhelming.

Trash containers should be removed from proximity to the cargo facility. This method of employee theft is common to most industry, but can prove particularly insidious to trucking as it is a convenient way to remove bulky cargo from the premise.

All employees should be subject to irregular inspection. The element of surprise is essential. This is one of the most effective ways to deter the "nickle and dime" thefts committed by dockworkers and other non-driver personnel that comprise the majority of losses.

Likewise, supervisors should not hesitate to recall a truck for recounting after it has left the premises. The essential responsibilities of supervision and crime deterrence are better assimilated with employee behavior if this type of spot auditing is imposed.

This latter alternative can be beneficial in the detection of driver involvement in thefts. Since drivers, particularly long distance operators, are on the road unsupervised for long periods of time, the opportunities for theft by these drivers are maximized, the control of theft presents a difficult problem. Most industry sources cite the necessity of reliance on the drivers, which can be developed through comprehensive pre-employment screening.

Although established to maximize safety potential of truckers on the highways, the Federal Motor Carrier Safety Regulations contain many provisions that minimize vulnerabilities to employee theft by drivers.

For example, primary among these requirements is a minimum hiring age of 21. Many carriers revise this minimum age upwards to 25 years to ensure an even greater amount of maturity and experience. Further helpful security controls involve requirements for written and road tests, and a requirement that a company perform a mandatory background check on qualifications and experience.

Pre-employment screening is integral to any internal policy and should follow the guidelines put forth in Section II. The Federal guidelines apply only to long-distance drivers; screening for intra-city must take special care to avoid hiring the "floater" driver. The nature of the employment -- with its opportunities for theft enhanced by the length of time unsupervised -- mandates special precautions. Despite the majority of walk-in applicants, management should not abrogate its responsibility to thoroughly check each applicant. A sample application for employment is included to illustrate a comprehensive form.

Industry sources also suggest that fingerprinting and other standard law enforcement tools be used at the application phase. Often hard-core criminals can be eliminated from consideration because they balk at such screening.

However, as indicated in Section II, many such tools are subject to stringent regulations as is the use of the polygraph, for example. A number of states prohibit its use entirely in a pre-employment situation.

Many carriers look at conviction records of applicants, if available. The motor industry cites the unavailability of criminal conviction records as a major stumbling block to effective cargo theft prevention. While cognizant of the limitations an individual's right to privacy places on the dissemination and use of such information, industry sources believe that entrusting freight and equipment worth thousands of dollars to individuals who possess criminal records for property theft and related offenses is contradictory and only aggravates the cargo theft problem. Toward the goal of reconciling the conflicts between privacy and protection, the motor industry has recommended that such information be used only for purposes of employment review, that it be limited to "conviction record information," that it be limited to the period of seven years immediately prior to the date of inquiry and that it be made available only on the written authorization of the individual whose records are sought.

Summary

Truck losses to crime have proven to be greatly reduced and minimized through implementation of policies of careful employment practices, conscientous supervision, and informed decisions on physical security of both the terminal and in-transit vehicles.

APPLICATION FOR EMPLOYMENT

ATA Form CO710. Reorder from
American Trucking Assns., Inc.
1616 P St., N.W., Wash. D.C. 20036

Applicant: Read and sign before submitting this application:

The Age Discrimination in Employment Act of 1967 prohibits discrimination on the basis of age with respect to individuals who are at least 40 but less than 65 years of age.

I understand that the information in this application will be used and that prior employers will be contacted for purposes of investigation as required by 391.23 of the Federal Motor Carrier Safety Regulations.

SIGNATURE OF APPLICANT ________________ DATE ________________

COMPANY ________________ STREET ADDRESS ________________

CITY, STATE AND ZIP CODE ________________

NAME ________________ (First) (Middle) (Last) PHONE ________________ SOCIAL SEC. NO. ________________

ADDRESS ________________ (Street) (City) (State & Zip Code) HOW LONG? ________________

ADDRESSES FOR PAST THREE YEARS
________________ (Street) (City) (State & Zip Code) HOW LONG? ________________
________________ (Street) (City) (State & Zip Code) HOW LONG? ________________

(ATTACH SHEET IF MORE SPACE IS NEEDED)

HT. ________ WT. ________ DATE OF BIRTH ________ (ANSWER ONLY IF APPLYING FOR DRIVING POSITION)

IN CASE OF EMERGENCY NOTIFY: ________________ (Name) (Address) (Phone)

POSITION APPLIED FOR ________________ TEMPORARY OR PERMANENT ________________

HAVE YOU WORKED FOR THIS COMPANY BEFORE? ________ WHERE? ________________

DATES: FROM ________ TO ________ RATE OF PAY ________ POSITION ________________

REASON FOR LEAVING ________________

NAMES OF RELATIVES IN OUR EMPLOY ________________

ARE YOU NOW EMPLOYED? ________ IF NOT, HOW LONG SINCE LEAVING LAST EMPLOYMENT? ________________

WHO REFERRED YOU ________________ RATE OF PAY EXPECTED ________________

PHYSICAL HISTORY

LIST ANY PHYSICAL LIMITATIONS (SUCH AS EYESIGHT, LIMB IMPAIRMENT, DIABETES, HEMORRHOIDS) ________________

____

ARE YOU PHYSICALLY CAPABLE OF HEAVY MANUAL WORK ________________

DATE OF LAST PHYSICAL EXAMINATION ________ DOCTOR'S NAME AND ADDRESS ________________

____

EVER INJURED ON THE JOB? ________ GIVE NATURE AND DEGREE OF SUCH INJURIES ________________

____

HOW MUCH TIME LOST FROM WORK IN PAST THREE YEARS FOR ILLNESS ________________

HAVE YOU RECEIVED WORKMEN'S COMPENSATION ________ WHEN ________________

EMPLOYMENT RECORD

NOTE: D.O.T. Requires that Employment for at Least 3 Years be Shown
(Attach Sheet if More Space is Needed)

LAST EMPLOYER: NAME ____________________

ADDRESS ____________________

POSITION HELD ____________________ FROM ________ TO ________ SALARY ________

REASONS FOR LEAVING ____________________

SECOND LAST EMPLOYER: NAME ____________________

ADDRESS ____________________

POSITION HELD ____________________ FROM ________ TO ________ SALARY ________

REASONS FOR LEAVING ____________________

THIRD LAST EMPLOYER: NAME ____________________

ADDRESS ____________________

POSITION HELD ____________________ FROM ________ TO ________ SALARY ________

REASONS FOR LEAVING ____________________

MILITARY STATUS

HAVE YOU SERVED IN THE U.S. ARMED FORCES? ________ BRANCH ____________ DATES: FROM ________ TO ________

RANK AT DISCHARGE ____________________ DATE OF DISCHARGE ________

(IN N.J. DO NOT FILL IN THIS LINE UNLESS HIRED) DRAFT STATUS ____________ RESERVE STATUS ________

EDUCATION

CIRCLE HIGHEST GRADE COMPLETED: 1 2 3 4 5 6 7 8 HIGH SCHOOL: 1 2 3 4 COLLEGE: 1 2 3 4

LAST SCHOOL ATTENDED ____________________
(Name) (Address)

GENERAL

LABOR UNION AFFILIATION (SHOW NAME OF UNION AND LOCAL) ____________________

HAVE YOU EVER BEEN BONDED ________ NAME OF BONDING COMPANY ____________________

HAVE YOU EVER BEEN CONVICTED OF A FELONY ____________________

HAVE YOU EVER BEEN KNOWN BY ANY NAME OTHER THAN THE ONE ON THIS APPLICATION ____________________

EXPERIENCE AND QUALIFICATIONS – DRIVER

	STATE	LICENSE NO.	TYPE	EXPIRATION DATE
DRIVER				
LICENSES				

A. Have you ever been denied a license, permit or privilege to operate a motor vehicle? YES ________ NO ________

B. Has any license, permit or privilege ever been suspended or revoked? YES ________ NO ________

C. Have you ever been disqualified subject to section 391 of the Federal Motor Carrier Safety Regulations? YES ________ NO ________
IF THE ANSWER TO EITHER A, B OR C IS YES, ATTACH STATEMENT GIVING DETAILS

DRIVING EXPERIENCE

CLASS OF EQUIPMENT	TYPE OF EQUIPMENT (VAN, TANK, FLAT, ETC.)	DATES FROM	TO	APPROX. NO. OF MILES (TOTAL)
STRAIGHT TRUCK				
TRACTOR AND SEMI-TRAILER				
TRACTOR – TWO TRAILERS				
OTHER				

LIST STATES OPERATED IN FOR LAST FIVE YEARS ____________________

____

SHOW SPECIAL COURSES OR TRAINING THAT WILL HELP YOU AS A DRIVER ____________________

WHICH SAFE DRIVING AWARDS DO YOU HOLD AND FROM WHOM? ____________________

ACCIDENT REVIEW FOR PAST 3 YEARS **(Attach sheet if more space is needed)**

DATES	NATURE OF ACCIDENT (HEAD-ON, REAR-END, UPSET, ETC.)	FATALITIES	INJURIES
LAST ACCIDENT			
NEXT PREVIOUS			
NEXT PREVIOUS			

TRAFFIC CONVICTIONS AND FORFEITURES FOR THE PAST 3 YEARS (OTHER THAN PARKING VIOLATIONS)

LOCATION	DATE	CHARGE	PENALTY

EXPERIENCE AND QUALIFICATIONS—MAINTENANCE

List courses and training in maintenance work

Indicate training and experience in the following:	**Training (Check)**	**Years of Experience**	**Area**	**Training (Check)**	**Years of Experience**
Drive Line Components			Body Work		
Diesel Engine Tune-up and Rebuild			Electrical Repair		
Gas Engine Tune-up and Rebuild			Frame and Wheel Alignment		
Tire Service			Brakes		
Trailer Repair			Cooling System		
Preventive Maintenance			Safety Line Checking		

Show equipment you can operate	**Training (Check)**	**Years of Experience**	**Equipment**	**Training (Check)**	**Years of Experience**
Woodworking Equipment			Wheel & Tire Balancing Mach.		
Sheet Metal Equipment			Tire Recapping Mold		
Frame & Axle Straightening E.			Engine Dynamometer		
Engine Rebuilding Equipment			Chassis Dynamometer		
Diesel Injection Equipment			Magnetic Crack Detector		
Electric Welder			Engine Analyzer		
Oxyacetylene Welder			Noise Measuring Equipment		
Paint Spray Gun			Smoke Measuring Equipment		

EXPERIENCE AND QUALIFICATIONS—CLERICAL

List courses and training in office work

Indicate training and experience in the following:	**Training (Check)**	**Years of Experience**		**Training (Check)**	**Years of Experience**
Typing*			Accounting		
Shorthand*			OS&D		
Billing			Interline		
TWX			Claims		
PBX			Cashier		
Key Punch Operator			Dispatcher		
Calculator			Tabulator		
Dictating Machine Transcriber			Mimeograph		
Bookkeeping Machine			Rates (Indicate tariffs with which you have worked)		
Adding Machine					
Other:					

*INDICATE WORDS PER MINUTE

EXPERIENCE AND QUALIFICATIONS — PLATFORM

LIST TYPES OF PLATFORM EXPERIENCE AND YEARS OF EACH

LIST PLATFORM EQUIPMENT YOU CAN OPERATE (LIFT TRUCK, ETC.)

SHOW COURSES OR TRAINING IN PLATFORM WORK

TO BE READ AND SIGNED BY APPLICANT

It is agreed and understood that any misrepresentations of information given above shall be considered an act of dishonesty.

It is agreed and understood that the employer or his agents may investigate the applicant's background to ascertain any and all information of concern to applicant's record, whether same is of record or not, and applicant releases employers and persons named herein from all liability for any damages on account of his furnishing such information.

It is also agreed and understood that under the Fair Credit Reporting Act, Public Law 91-508, I have been told that this investigation may include an Investigating Consumer Report, including information regarding my character, general reputation, personal characteristics, and mode of living.

I agree to furnish such additional information and complete such examinations as may be required to complete my employment file.

(Massachusetts, Georgia & Kansas only) — I understand that, as a condition of employment, I will obtain from the Registry of Motor Vehicles, within my probationary period, and without cost to the employer, a copy of my motor vehicle violations record.

(Pennsylvania only) — I authorize my employer to obtain from the Registry of Motor Vehicles a copy of my Motor Vehicle Violations Record.

It is agreed and understood that this application for employment in no way obligates the employer to employ me; and it is understood that if hired, I may be on a probationary period during which I may be discharged without recourse.

This certifies that this application was completed by me, and that all entries on it and information in it are true and complete to the best of my knowledge.

Date   Applicant's Signature

"Under Maryland law an employer may not require or demand any applicant for employment or prospective employment or any employee to submit to or take a polygraph, lie detector or similar test or examination as a condition of employment."

Date   Applicant's Signature

APPLICANT — DO NOT WRITE BELOW THIS LINE

PROCESS RECORD

APPLICANT HIRED REJECTED

DATE EMPLOYED POINT EMPLOYED

DEPARTMENT CLASSIFICATION

(IF REJECTED, SUMMARY REPORT OF REASONS SHOULD BE PLACED IN FILE)

THIS SECTION TO BE FILLED IN BY RESPONSIBLE OFFICER OR COMPANY REPRESENTATIVE

	SUPERIOR	GOOD	FAIR	BELOW AVERAGE	POOR	WRITTEN RECORD ON FILE
1. APPLICATION						
2. INTERVIEW						
3. PHYSICAL EXAM						
4. PAST EMPLOYMENT						
5. WRITTEN EXAM						
6. ROAD TEST						
7. POLICE AND TRAFFIC RECORD						

SIGNATURE OF INTERVIEWING OFFICER

TRANSFERS

FROM: TO: FROM: TO:

DATE: DATE:

REASON FOR TRANSFER REASON FOR TRANSFER

TERMINATION OF EMPLOYMENT

DATE TERMINATED DEPARTMENT RELEASED FROM

DISMISSED VOLUNTARILY QUIT OTHER

TERMINATION REPORT PLACED IN FILE SUPERVISOR

Air Cargo

Air transportation of cargo traditionally has received secondary attention to passenger transport by the regularly scheduled airlines. As a result, this industry, which had total revenues of approximately $1.2 billion in 1975, has developed erratically, but rapidly.

Specializing in the transport of high-value/low volume cargo, air transport is more expensive than trucking, rail or maritime. Although it transports more, in terms of value of goods, air cargo is still the smallest sector, in terms of absolute volume, among the modes of transportation.

Air cargo transportation is a highly concentrated industry. Over 70 percent of the value of cargo transported is handled through six locales: New York, Los Angeles, Chicago, Miami, San Francisco and Boston. Of the group, New York's three metropolitan airports handle almost 30 percent.

An unfortunate by-product of the exponential growth of air freight in the past decade was a corresponding crime explosion. A primary reason was the delayed growth of facilities to accommodate the upsurge in cargo. The lack of sufficient facilities exposed cargo to inadequate storage and handling and to theft and damage. Losses peaked in 1969-1970 when a maritime strike accentuated already chaotic conditions; losses totalled $13.8 million.

Since the 1969-1970 strike and the Senate Select Committee on Small Business hearings, carriers have expanded facilities and improved cargo-handling techniques. Losses have declined to a point where air cargo transportation claims lower losses than other carriers.

Dollar Losses

Losses incurred by the air cargo sector as a result of theft are reflected by a claims ratio which measures the amount paid out in claims for every $100 in revenue. This ratio decreased from 1.40 percent in 1971 to .84 in 1975. The total loss, in 1975, was $10.5 million. According to the Air Transport Association (ATA), theft-related claims were 53 percent or $5.5 million, while damage/delay amounted to 47 percent or $5.0 million. Theft-related claims, as a percent of total, have been significantly reduced since 1970. In that year, theft-related claims were paid in 66 percent of the cases.

The trend in air cargo is toward loss reduction. From 1970-1975, total revenues increased 78 percent, total claims paid decreased 24 percent, and the loss ratio decreased 55 percent.

Losses result from factors other than crime. Air cargo transports a large volume of perishables and if shipment is delayed, and perishables damaged, it results in an ultimate loss to the airline responsible for the delay. Cut flowers make up a sizeable segment of perishables; they represent the third leading loss category to airlines -- claims paid for loss of this commodity were $647,000 in 1975, an increase of 4 percent over 1970.

Vulnerabilities

The high-value/low volume nature of air cargo increases the risk of theft.

ATA data indicate that wearing apparel, electrical equipment, jewelry, watches and clocks are key targets for thieves. Claims for wearing apparel decreased, however, 40 percent from 1970-1975. Claims for electrical equipment, on the other hand, increased 23 percent.

Vulnerability to theft is greatest while the merchandise is in the terminal awaiting further shipment or final delivery pickup by truck. Anti-hijacking measures all but eliminate loss in transit.

Theft varies among terminals, and the function of the terminal can be a primary factor in determining the extent of theft. International terminals tend to resemble warehouses, with shipment delays of several days, whereas domestic terminals are primarily transfer points, where merchandise moves quickly.

Although there is an increased potential for crime in international terminals, due to the extended storage of goods, this risk is somewhat offset by Federal regulations governing international shipments. The U.S. Bureau of Customs considers an international terminal to be a bonded warehouse. As a result, there is greater control. Customs requires a "manifest" -- a list of shipments -- which is transported separately from the shipment. This eliminates the ease of altering a manifest to cover up thefts. Moreover, the mere existence of the manifest deters crime because it enables quick checking of the list against contents, to spot discrepencies.

Theft potential also varies among airlines as a result of individual warehousing techniques. Material handling techniques are of utmost importance in reducing theft. Cargo managers who do not practice efficient warehousing methods are susceptible merely because the merchandise is not stored in an orderly fashion.

Employee Theft

Theft and pilferage of cargo is usually committed by persons authorized to be on the premises, using vehicles authorized to be there. A study of New York Metropolitan airports indicated that 76 percent of all losses were committed in this manner, and that 70 percent of these losses were thefts from terminals. This same study showed that armed robbery and hijackings were rare, comprising only one percent of thefts, but the value of those rare exceptions accounted for 25 percent of losses. This situation corresponds to trucking transportation.

Prevention

While cargo security in air terminals is a function of good operating procedure, it is clear that cargo transporters benefit greatly from anti-hijacking measures that are mandatory for airlines. Cargo also has among the most sophisticated security -- at least one carrier at New York's JFK cargo terminal is entirely computerized. Theft prevention has been aided, as well, by containerization, and the development of wide-bodied jets that have given additional impetus to the utility of unit load devices. Cargo can now be transferred from the customer to the container to the plane with minimal exposure. Entire containers are rarely stolen.

The theft that remains results almost exclusively from inefficient operating procedures -- for example, poorly implemented physical security, non-recognition of technological developments or basically poor management-employee relationships.

Efficient operating procedures are thus mandatory to reduce crime losses. Exposure makes the theft possible, and inefficiency increases exposure. Reduction of losses is imperative, as it is becoming more evident that a shipper chooses a particular carrier at least partly on reputation for claims prevention.

Efficient operating procedures that reduce crime losses contain at least three elements: utilization of storage techniques and special handling procedures for high value cargo; system of record-keeping; and employee controls.

Storage techniques build on basic warehousing concepts. For example, racks are necessary to keep cargo off the floor in easily identifiable locations. Cargo cannot remain on the floor uncategorized. When storage is lax or sloppy -- losses occur -- both through theft and damage.

Bins or separate storage areas for high-value cargo should be maintained. Most carriers do have separate rooms equipped with locks and alarms. Some carriers add to this protection by installing safes within these locked rooms for extra-sensitive cargo, such as jewels or bullion. This policy should supplement a basic policy calling for movement of sensitive cargo into storage or into delivery as quickly as possible. The less time the high-value cargo remains in the terminal -- the less exposure to theft.

High-value cargo is better protected if its nature is noted on the manifest. For example, to control intracity transfer of high-value shipments, ATA interline procedures require a "high-value" notation in the remarks section of the transfer manifest.

The use of over, short and damage (OS&D) reports as the basic record-keeping tool of management assists in pinpointing areas of excessive loss. A sample of one carrier's report form follows.

The potential of the OS&D as an early-warning system to detect losses is significant. As a current, continual record of activity, it becomes an effective auditing tool as well.

Currently, the majority of the industry uses the filed claims form to keep record of claims payments, rather than the OS&D. This after-the-fact record keeping has little deterrent value. The use of the OS&D, on the other hand, enables analysis and trend discernment before claims multiply.

Within the industry, effective approaches to security vary widely. They range from utilizing loss prevention specialists to a computerized cargo system that incorporates loss prevention into its operating procedures. An illustrative case study is included in this study that highlights a loss prevention program.

On an airport-wide basis, the most progressive example of airport security is the 8 year old Airport Security Council of the New York Metropolitan airports. The New York Airport Security Council is one among 50 security committees established by the ATA at airports throughout the country. The innovations -- both physical security and internal control -- in airport security have been widely copied elsewhere.

Summary

The relative success in loss reduction in the cargo transportation industry is traceable to several factors. The size of the industry; the minimal threat of in-transit loss; and the

Airport Security Council and ATA research are primary factors. However, the cooperation of individual carriers in implementing loss prevention procedures and initiating deterrent policies has been fundamental.

Sources:

1. Air Transport Association of America
   1709 New York Avenue, N.W.
   Washington, D.C. 20006

2. Airport Security Council
   Lefrak Tower
   97-45 Queens Blvd.
   Forest Hills, New York 11374

3. <u>Air Freight Loss and Damage Claims</u>
   Department of Transportation
   800 Independence Ave., S.W.
   Washington, D.C.
   202-426-4828

□ AIR FREIGHT INSPECTION
□ WAIVER OF INSPECTION
□ AIR FREIGHT LOSS OR DAMAGE

FREIGHT INSPECTION AND CLAIM

ABG 70530
OPR-253
REV. 3/73

AIRBILL NUMBER	AIRBILL DATE / /	CLAIM NO.

SHIPPER'S NAME AND ADDRESS

DECLARED VALUE □ $ AMOUNT
SHIPPER'S INS. □ $

CONSIGNEE'S NAME AND ADDRESS

DATE INSPECTION REQUESTED / /	TIME	INSPECTION DATE / /	TIME	WHERE INSPECTION MADE?

NO. PCS. SHIPPED | WEIGHT | NO. PCS. □ SHORT □ DAMAGED

CONTENTS

COMMODITY DESCRIPTION

MARKS AND LABELS
□ THIS END UP □ GLASS □ CONTENTS INDICATED
□ FRAGILE □ DO NOT LAY FLAT □ HANDLE WITH CARE
□ OTHER (DESCRIBE)

GROSS WEIGHT LIMIT OF CONTAINER

ACTUAL GROSS WEIGHT OF CONTAINER AND CONTENTS

DELIVERY
□ CONSIGNEE PICKED UP □ HEATED CARGO SPACE
□ CARTAGE AGENT □ CLOSED TRUCK
□ OPEN TRUCK

DATE OF DELIVERY

INDEPENDENT TRUCKER'S NAME

CITY

Could consignee have noticed any damage to shipment (wet, crushed, rattle, etc.) at time of delivery and before unpacking? □ YES □ NO

If YES, did consignee note exception on delivery copy of airbill? □ YES □ NO

Were damaged items and packaging available for inspection? (If not, explain on bottom portion of copies 3 and 4.) □ YES □ NO

NUMBER AND DESCRIPTION OF ITEMS (MAY ITEMIZE ON REVERSE)

□ SHORTAGE
OR
□ DAMAGE

CONTAINER WEIGHT WHEN SHIPPED	WAS THERE SPACE FOR MISSING ITEMS? □ YES □ NO	CONTAINER WEIGHT ON DELIVERY	SHORTAGE VERIFIED BY INVOICE □ YES □ NO

OUTER PACKING
□ CORRUGATED CARTON
□ CARDBOX BOX
□ PAPER WRAPPED
□ WOOD BOX
□ WOOD CRATE
□ METAL CAN
□ BARREL
□ BUNDLE
□ NONE
□ OTHER ______

CONTAINER DETAILS
□ CORDED
□ TAPED
□ GLUED
□ STAPLED
□ BANDED
□ LOCKED
□ OTHER ______
□ NEW
□ USED

CONTAINER DEFECTS

Outer		Inner
□	TORN	□
□	PUNCTURED	□
□	CRUSHED	□
□	SEAMS OPEN	□
□	BANDS LOOSE	
□	WET	□
□	STAINED	□
□	DENTED	□
□	RECOOPERED	
□	NO DEFECTS	□

INNER PACKAGING
□ CORRUGATED LINERS
□ CORRUGATED DIVIDERS
□ EXCELSIOR
□ SHREDDED PAPER
□ CRUMPLED PAPER
□ WOOD BRACING
□ FITTED CASE
□ INDIVIDUAL BOXES
□ BOTTLES – JARS
□ OTHER ______

MERCHANDISE WILL BE
REPAIRED □ SALVAGED □ USED AS IS □ SCRAPPED □ RETURNED TO SHIPPER □

EST. REPAIR COST $	SALVAGED VALUE $	INVOICE VALUE $	SCRAP VALUE $

SEE REVERSE SIDE FOR DIAGRAMS, COMMENTS, ETC. □

EA INSPECTOR'S SIGNATURE		CONSIGNEE'S (OR HIS AGENT'S) SIGNATURE	DECLARED VALUE $
EA ADDRESS CODE	DATE AND TIME / /	SIGNER'S JOB TITLE	SHIPPER'S INSUR. $

THE ABOVE REPORT IS NOT A CLAIM NOR LEGAL NOTIFICATION OF INTENT TO FILE CLAIM – SEE BELOW

CLAIMANT'S NAME AND ADDRESS

CLAIMANT'S CLAIM NUMBER

TO FILE A CLAIM, SEND
- THIS FORM COMPLETED
- □ ORIGINAL INVOICE FOR GOODS LISTED BELOW
- □ INVOICE FOR REPAIRS
- A COPY OF AIRLINE AIRBILL

TO: Eastern Air Lines, Inc.
Customer Relations/
Freight Claims, Bldg. 5-A,
Miami International Airport
Miami, Florida 33148

LOSS, DAMAGE REPORTED TO: EASTERN REPRESENTATIVE LOCATION

DATE / /

COMMUNICATED BY □ PHONE □ WIRE □ ______

GOODS LOST OR DAMAGED			DETAILED REASON FOR CLAIM	AMOUNT OF CLAIM
NO.	UNIT	DESCRIPTION		
				$

SIGNATURE OF CLAIMANT OR CLAIMANT'S REPRESENTATIVE	JOB TITLE OF CLAIMANT'S REPRESENTATIVE	DATE / /	TOTAL AMOUNT OF CLAIM	$

1 | Distribution for: LOSS OR DAMAGE Return to Origin Station | Distribution for: INSPECTION to Consignee | Distribution for: CLAIM, forward to: ⟶ (with supporting documents)

CASE STUDY: AIRPORT COMBINED RESOURCES OF MEMBER AIRLINES TO IMPLEMENT SUCCESSFUL CRIME LOSS REDUCTION PROGRAM

Background: This case study describes a highly effective security program developed to cut sizeable cargo value losses at a major U.S. airport. Nearly 50 percent of the value of all international cargo entering the United States is handled at this airport, which is more than is handled at all other U.S. airports combined. Moreover, together with three other regional airports, the subject facility handles almost one-third of all cargo -- domestic and international -- handled at U.S. airports. Tonnage handled at the airport approximates 1 million tons annually, the value of which exceeds $15 billion.

Approximately 45 airlines use the airport. All but a few carry cargo as a secondary function after passenger transport, although the major carriers operate individual cargo-handling facilities in areas away from the main passenger terminals. A major U.S. departure and entry point, the complex is quite large.

The impact of the maritime strike in 1969-70 on this airport was severe because its location made it adaptable to receipt and transfer of international cargo. The strike, combined with the explosive growth in overall demand for air cargo, caught the airport management unprepared to accommodate the influx of cargo. This situation, in light of the airport's promixity to a metropolitan area with a legendary crime rate, exposed the facility to skyrocketing losses.

Problem: The airport was experiencing major losses; in 1969, cargo valued at $3.4 million was lost.[1/]

Major thefts ($20,000 or greater) occurred infrequently, although the value of cargo stolen in an average major incident was of such magnitude that these thefts accounted for approximately half of all losses. Pilferage and minor thefts -- average loss about $2,000 -- was a recurring problem. Armed robberies

[1/] All data are aggregates. Technically, it is not the airport that suffers from crime loss -- it is the individual airline. However, individual airlines do not release loss data.

and hijackings occurred even less frequently than major thefts, but were still a significant source of loss. In 1969, there were only 3 armed robberies.

The table below summarizes the major types of crimes at the airport during the period 1969-1974.

Crime	Number of Incidents	Loss as Percentage of Total Dollar Loss
Major theft	85	57
Armed robbery (hijacking)	12	21
Minor theft	1,943	22

Three-fourths of reported losses occurred within the cargo terminal and were suspected employee theft -- that is, theft by persons authorized to be on the premises, using vehicles authorized to be there. Analyses of the weight of missing cargo -- 52 percent exceeded 50 pounds -- indicated that most left the terminal on trucks in the guise of normal cargo movement. Target items were high value, low volume: currency, furs, jewelry, watches, precious metals and precious stones. These six items alone comprised two-thirds, by value, of all cargo losses.

Objective: Security programs were designed to reduce geometrically expanding crime losses on a cost-effective basis, without limiting the flexibility required in a highly competitive industry undergoing rapid growth.

Steps Taken: Each of the 45 airlines using this airport has its own security program, predicated on individual needs. However, much of the substance of these individual programs is derived from participation in an Airport Security Council (ASC). This ASC was established by the airlines and is one of 50 similar councils at airports throughout the country. It was designed essentially to be a managerial and consulting organization that would develop programs and procedures for implementation by member airlines. Its operating philosophy focuses on being the "cohesive agent to utilize the maximum resources of the carriers for mutual benefit of the industry."

The council is governed by an Executive Committee composed of member airlines. While some proposals developed by ASC are not necessarily applicable to each airline terminal and are advanced only as recommended procedures, many are universally suitable and are mandated for use by all member airlines. The Executive Committee established a policy subjecting member airlines to possible fines if they failed to comply with mandates.

The initial mandate was the development of a theft reporting system; all council members are required to record thefts, pilferages, and losses of cargo under the ASC Uniform Reporting System. These data are reported to appropriate law enforcement agencies and to the ASC. The analysis of loss reports enables development of the data described in the Problem section, above. Findings have been determined by the ASC to be the key to the problem solution. Analysis provides critical data on incidents and values, to assess costs of losses, and more significantly, details concerning the "what, where, when, why, and how" of losses at the airport. Specifically, the loss analysis identifies theft-vulnerable commodities; pinpoints vulnerable areas; isolates vulnerable times and specifies weak points in operating procedures.

(1) Personnel

Since three-fourths of crime losses have been identified as employee-caused, major emphasis has been directed to developing employee controls.

The initial development was a mandated employee identification badge system, to restrict accessibility of the terminal areas to authorized personnel. This system functions to eliminate the problem created both by the size of the terminal areas, and the difficult logistics of unloading and loading shipments in a short period of time.

Employee identification is a fundamental management control that enables a greater degree of accountability in the case of an actual theft, and generally enables management to exert a greater degree of control by visually separating authorized personnel from non-authorized personnel.

The badge system initiated by the ASC has been implemented by the individual airlines, and enforcement is the responsibility of the airline security personnel. Implementation of the system has been almost 100 percent effective. Members, again, are subject to fines if they do not comply with the mandated measure.

The second major development was a cargo employee central index, for use by carriers in personnel selection. This system, developed in cooperation with law enforcement, has been designed to facilitate and encourage background checking of applicants. As in many industries, preference in hiring has been given to applicants with prior cargo-handling experience; moreover, experience frequently has been the sole selection criterion. However, as many other service industries have discovered, a "floater" problem results from such hiring practices. The central index helps eliminate this type of problem, by reducing the expense and time involved in background checking.

A third major effort has been a reward program for information about cargo thieves. Specifically, standing offers of cash rewards for information leading to arrest and conviction of persons involved in theft or pilferage of air cargo on the premises of a member are posted at strategic areas in cargo operations.

Other standard security precautions have been recommended by ASC and mandated by the airlines. For example, airlines must designate prescribed parking areas adjacent to the cargo terminals and segregate employee parking from operating areas, to eliminate pilferage.

(2) Operating

This is the area in which the impact of ASC has been most effective. Two distinct programs were envisioned: (1) issuance of principles of physical security, tailored to specific vulnerabilities of specific terminal areas and cargo; (2) the issuance of advisory opinions concerning installation, effectiveness, or maintenance of physical security devices.

Both programs have been developed and, without exception, have taken into consideration the cost of security in relation to the value of the items to be protected. Many operational initiatives have been, as a result, relatively simple, reflecting management awareness that effective security does not necessarily mean expensive security.

Examples of operational security measures identified by ASC and mandated by member airlines include erection of barriers or painting of lines to separate public terminal areas from segregated areas -- beyond which only authorized persons (identified by the above-mentioned employee badge system) are allowed. An accompanying mandate provides that airlines may not stow or leave cargo unattended in front of these barriers. These two measures have minimized opportunities that truckers formerly had to steal cargo. Prior to implementation of the requirement, there was no clearly defined separation of areas, and movement of cargo in and out was unorganized and haphazard. The access to cargo that truckers -- who were usually indistinguishable from airline employees -- had in this type of structure simplified cargo theft.

To further reduce the potential of trucker thefts and cargo employee-trucker collusion, additional mandated measures have been adopted. Airline employees are prohibited from releasing cargo -- or documents -- to anyone without a full identification of the recipient. Airlines, moreover, are required to use a specific airport form for imports which is designed to prevent fraudulent pickup. Also, platform doors in cargo terminals are to be closed when not in use.

A significant component to improved operating security has been the development of strict, specific procedures for the protection of high-value cargo. This action has been imperative, in light of the identification of commodities that are theft targets -- high value, low volume. The basic approach to high-value cargo is founded on a "move it out quickly" philosophy -- the shorter the length of time that the theft-attractive cargo remains in the terminal awaiting shipment, the more theft opportunities are reduced.

High-value bins are used to expedite the movement of this cargo. High-value cargo is identified on the shipping manifest, and transferred to the bins. An argument against handling high-value cargo in this fashion is that it becomes clearly identified, and thieves could more easily zero in on the desired targets. This situation has been minimized, however, through application of operating security guidelines established by the ASC.

For cargo that cannot be moved as quickly as security mandated, additional protection has been devised: high-value storage. In at least one airline cargo facility, there are 4 layers of protection in high-value storage: (1) a locked cage which surrounds, (2) the locked storage room, (3) which is guarded by a security employee and (4) in the case of truly high-value cargo -- bullion, gems -- it is further protected by a locked safe.

Individual airlines have implemented additional methods of safeguarding high-value cargo: a prominent example is the procedure whereby origin stations notify destination terminals of incoming high-value shipments. This step alerts cargo handlers to the need for special protection.

Results: In 1975, [2/] net loss from cargo theft at this airport was valued at $594,000. Gross loss was $1.4 million; $795,000 was recovered. In contrast, in 1969, net loss was valued at $3.4 million. Gross losses for that year were valued at $3.9

[2/] Figures have been rounded.

million. Recovery amounted to $500,000. The reduction in gross losses, after introduction of security measures, is significant.

These sharp reductions -- nearly two-thirds in gross losses and over 80 percent in net losses -- underscore the effectiveness of the deterrent program designed by ASC and implemented by the member airlines. Moreover, they illustrate the effectiveness of the prosecution policy: in 1969 the value of recovery of stolen cargo by law enforcement equalled only 13 percent of gross cargo stolen. In 1975, that ratio exceeded 50 percent.

Significantly, the ASC reports valuable support from public law enforcement and other agencies in the fight against cargo theft. The airport police gave good insight into the causes of crime, and pertinent counter-measures, as far back as 1968. Increased patrols, assigning of investigators to specific airlines, and the organization of a monthly meeting of security and police officials, contributed to the ultimate success of the program.

The ASC cites the following results of law enforcement support relating to cargo theft at the airport: 6 percent of minor thefts and 25 percent of major thefts have been solved through arrest. There have been 412 arrests -- 35 percent of which were employees. These data are significantly higher than national arrest figures for other crimes. Larceny arrests, for example, are less than 1 percent of crimes reported.

Reduced crime losses not only mean reduced claim payments, but also such indirect benefits as more favorable reputations for those airlines who have significantly reduced their losses. Shippers and/or receivers do not want to entrust their cargo to an airline unable to protect it from thieves.

Airlines with low crime loss rates save the expense and employee time involved in handling claims. Although there are no statistical estimates covering the cost of handling claims, these costs must significantly increase the overhead of an airline.

A more important, although intangible, benefit to the airport, accruing from a successful security program, is the ability of an airline to continue to expand services in response to a growing demand, knowing that crime is under control. The straightforward measures used by this airport in this case study, moreover, did not impact on the flexibility required in the industry. Rather, the program has been cited as improving the overall efficiency of operating procedures -- which is what an effective security program should accomplish.

CHAPTER 2

EDUCATIONAL SERVICES

Education is the largest item in State budgets, accounting for 39 cents of every budget dollar expended. Nevertheless, a majority of the 91,000 public elementary and secondary schools in the United States are facing financial crises. Expenditures per pupil in average daily attendance have more than doubled in the past decade, rising to $1,200 in 1974-75 from about $485 ten years ago.

Although many factors contribute to the worsening financial crisis, the penetrating scrutiny of city taxpayers is often responsible for cut budgets.

The conflict between rising costs and smaller budgets is manifested by austerity programs -- cafeteria closings, curtailment of music and art programs, elimination of summer school enrichment programs, cutbacks in maintenance services, or reduction in athletic programs.

Education expenditures nationwide are inflated by an estimated $600 million annual loss to crime. Crime has impacted not only on disciplinary problems in an educational sense, but on facility and equipment supply, without which education cannot function. In some school districts, crime costs as much as $7 million annually, when security costs are included. The damage is in the diversion of educational dollars from productive programs to loss and violence prevention -- from primary purposes to non-educational purposes.

Crime in and against schools always has been of intense concern to communities and to local, state and federal governments. This concern has been generated largely by the predominantly sociological origins of the crime, and has overshadowed the economic impact of the crime. Only within the past few years has the asset loss achieved equal attention to the larger sociological problems.

The fact that schools are ready targets for both juvenile delinquents and professional thieves is well established. Several theories exist as to why schools suffer such severe losses and why these losses have soared in this decade.

A primary factor is the increasingly developed facilities within the schools. Schools are literally gold mines for the thief. There are few schools not equipped with the latest in teaching aids: audio-visual, video tape, computers, business machinery, microfilm, photography labs, musical instruments, and a plethora of other vocational equipment.

All these items are high-value, low volume; they are in short, what attracts thieves. The loss is compounded for a school because the item is not easily replaced; the budgetary crunch facing schools often means the class learns with six typewriters instead of twelve.

The increasing size and changing structures -- both architecturally and internally -- of schools have contributed to crime problems. As educational philosophies have evolved, learning and environments have become more relaxed. Schools frequently resemble college campuses, and frequently, students enjoy freedom of movement about that campus. The opportunity for crime has been magnified by the informality and lessened supervision over students.

Student activism is a contributing factor. Students now actively seek redress against what they feel are unjust restrictions, dress codes and hair length codes, for example. Some experts believe that this activism creates an environment conducive to explosions.

Student drug abuse is another influencing factor. Recent surveys indicate that a trend toward increasing drug use by youths is in evidence after a declining level in recent years. However, in the years drug use declined, alcohol became a problem in many schools.

The National Education Association estimates that drug-related crime increased 81% from 1970-1975; and that 30 percent of the 18 million secondary school students use illegal drugs. Nationwide, there is no question among educators that drugs have been an important causative factor of increased stealing. Schools are ripe territory for drug pushers -- testimony before the Senate Subcommittee to Investigate Juvenile Deliquency revealed that daily drug sales of more than $2000 were not uncommon and that drugs in use ranged from marijuana to heroin.

Sociological factors remain one of the major causes of crime losses in this sector. Fundamental changes in lifestyles and values have placed substantial burdens upon educators who must attempt to guide youth into productive channels of society. The vital role the schools play often backfires as resentful youth take vengeance on the schools as a symbol of their failures.

Vulnerabilities and Losses

There are two broad loss areas within schools: personal violence and property crime. Crimes range from bomb threats, sex offenses, arson, school bus hijackings, assaults and murder -- to vandalism, burglary and robbery. Especially among the property crimes, there is frequently no clear definitional distinction between one crime and another. For example, arson can be a cover for burglary, and vandalism can be a by-product of theft. School administrators themselves frequently have no standard on which to differentiate between the crimes, which makes standard reporting and loss measurement difficult.

Although person-to-person crime -- assaults, murders, rapes -- has more psychological impact, property crimes far outweigh them in economic terms. The National Association of School Security Directors estimates total 1974 losses at $594 million. Losses broken down are shown in Table III.

TABLE III

1974 Losses, by Type of Crime[1]

(Millions of Dollars)

Burglary	243.0
Arson	109.0
Vandalism	102.1
Other	140.0
Total	594.1

Significantly, these losses do not account for the crimes that go unreported by administrators for fear of embarrassment from adverse publicity. For instance, in one case a $40,000 vandalism was "covered-up" by a principal to avoid the blame. In New York City, the rate of unreported incidents is estimated to be as high as 60 percent. Further, the Senate Subcommittee found that many schools did not even keep records of incidents; the National Association of School Security Directors supports this general observation.

[1] Burglary is standard breaking and entering, composed primarily of equipment theft.
Vandalism is malicious destruction.
Other includes larceny, window breakage, locker theft and other miscellaneous crimes.

As reflected in the above figures, burglary is the most costly crime. This is so because of the value and temptations of the "loot" inside the schools. Burglary is thought to be committed primarily by the professional as opposed to the amateur, since burglary of schools is highly lucrative and the prevalence of fencing operations ensures a ready market for the professional.

Fire loss is high in comparison to actual incidents, because of the expensive nature of fire. The National Fire Protection Association estimates that in the three year period 1968-1971, the number of school fire incidents increased from 10,600 to 15,700 with losses rising from $45 million to $72 million annually. Arson is the crime with the greatest damage potential; for example, in Alexandria, Virginia, an entire school was destroyed by an arsonist. The school was abandoned.

The losses from one incident are normally extremely high. The library of a high school in Washington was destroyed by an arsonist set fire and damages were $1 million, exclusive of book replacement cost.

Vandalism impacts in many areas within a school: from graffiti to malicious destruction of entire portions of the building. Exact losses stemming from vandalism depend on definitions of vandalism, as mentioned above. Vandalism -- malicious destruction -- resulted in losses of $102 million in 1974.

Recurring crime losses result from window and door glass breakage. Broken windows were a problem in over 90 percent of school districts contacted by the Senate Subcommittee. Although it is difficult to ascertain a peak in this crime, it is certain that eventually, losses will decline or be eliminated as glass is replaced with unbreakable substances. Currently, a 1975 School Product News survey estimates that reporting school districts spent an average of $9702 on glass breakage. At the same time, the survey found that 44 percent of respondents used vandal resistant windows, at an average cost per district of $8500. Since glass windows and doors serve as access into the facility, breakage is often a prelude to more serious losses stemming from theft, malicious destruction, or arson.

Bombings -- actual and threatened -- pose significant problems to schools. As with any bomb target, the reason for its selection as a target -- i.e. maximum exposure -- is also the reason why the bomb and bomb threats pose such significant problems.

Through the first nine months of 1976, schools ranked fourth among 23 selected targets on the FBI bomb compilation report. Damage in 1975, according to the FBI Annual Bomb Summary, was $833,602 for 165 bombings. Another cost, in addition to actual and attempted bombs, are bomb threats. Although the FBI no longer compiles data on threats, in 1973, there were 7,000 telephones threats; one telephone bomb threat can cost one city, for police and fire response, $2,000-$3,000. The motives for more than 75 percent of the bombings are malicious destruction, personal animosity, civil rights and anti-establishment.

Although crimes of personal violence occur less frequently than property loss, schools remain susceptible to crimes against personnel, teachers, other personnel, and students. Table IV, below, shows an estimate of incidents compiled by National Association of School Security Directors.

TABLE IV

1974 Incidents, by Type of Crime

Armed Robberies	12,000
Aggravated Assaults	204,000
Forcible Rapes	9,000
Burglaries	270,000

The impact of violent crimes extends beyond concise measurement. It must be measured, rather, in terms of the disruption to the learning process and the effects that a climate of fear and apprehension have on student morale. In some schools, students are afraid to use the restrooms for fear of assault. There are many instances, as well, of teachers being assaulted before or after school in their classrooms.

Cost of Security

Schools, like the business community, face increasing costs for security. The escalation results primarily from initial implementation necessitated by increasing losses. Los Angeles, for example, spent $3 million in a 3-year period on intrusion alarms. New York City, as long ago as 1971, spent $4.8 million on police and security guards in schools. One California school district with 60,000 average enrollment and 100 buildings, expended $126,000 for a system including personnel, equipment and alarms. The twelve silent alarms, alone, represented $75,000. Annual operating costs are $350,000.

Results of the 1975 survey conducted by School Product News into the average cost of school security are reflected in

Table V. Most commonly employed among responding schools were guards -- both in-house, contract and pseudo-guards (custodians); 41% used this type of security. Intrusion alarms and detectors were reported by approximately one-third of respondents. Four percent used vandal resistant windows -- primarily plastic glazed.

TABLE V

1974 Average Cost of Security

Type of Security	Average Expenditure Per District Reporting
Guards	$37,581
Intrusion Detectors	12,745
Intrusion Alarms	7,427
Vandalism - Resistant Windows	8,492

As with any security program, the initial costs of implementation are absorbed as crime losses are avoided. Some estimates indicate that installation of alarms, for example, has the capability of reducing vandalism by 90 percent. On the other end of the spectrum, the 1971 New York City expenditure of $4.8 million on security personnel did not prevent concurrent vandalism loss of $3.7 million.

Crime Prevention

There are two fundamental approaches to reducing losses within schools -- physical security and individual problem solving. The majority of the nation's 16,000 school districts use various combinations -- that is, applying physical security while attempting to address those specific student problems that might result in crime.

Regardless of which method -- or what combination -- is used by a school district, the security program must be subtle as it should be in any service industry. Security experts stress that crime prevention should not intrude on students, but rather, that it can and should be adapted to the educational environment. However, if the strategies do not blend with the educational purpose, and become obvious, they are likely to increase crime potential by generating additional hostilities and pressures.

Many educators assert that crime prevention techniques are inconsistent with education, in that learning is difficult to achieve in a climate of overt security. The hesitancy to resolve this inconsistency has resulted in increasing losses to crime. Experts who stress the importance of crime prevention in schools argue that educational purposes are more consistent with properly tailored security than with vandalism, theft or personal violence. This clearly appears to be an appropriate approach, and is one an increasing number of school districts are opting for.

Crime prevention methods will not achieve maximum effectiveness until educators become more fully aware of the problem. A significant barrier to decreasing crime's impact is the inability of educators to deal with it. Frequently identified by industry sources as an area in need of major improvement, teachers and administrators are ill-equipped to handle serious crime.

To equip teachers to cope with crime, one suggestion has been to orient them to crime and deterrents in the course of their professional training -- both in universities and refresher workshops sponsored by State or national educational associations. Absent this type of training, school districts should advise incoming teachers of local crime problems that often are a function of the community itself. Familiarity with local and State laws should be stressed so as to acquaint those who must deal with crime with what constitutes a crime. In this fashion, effective, comprehensive programs that will address major problem areas can be developed. Failure to recognize and cope with crime in schools has the same ramifications as does toleration of crime in other business sectors; it breeds more crime.

Deterrence through Individual Student Problem Solving

Many educators believe that an individual approach instills greater interest in the student of school, thus reducing the individual's hostilities that often result in crime by isolating and resolving the problems underlying those hostilities. An example is the discovery that a hostile high school student can't read beyond a primary grade level; correction of that problem often alleviates the potential danger which the student presents. Briefly, the student should be oriented toward productive conduct through peer group pressure, community involvement, and recognition that a traditional format is not necessarily ideal for all students, for example. Alternative programs should be established to provide an outlet for those students "ill-at-ease" in academic environments. In other words, efforts should be exerted to reach maximum number of students.

Treatment of disciplinary actions should be carefully structured. For example, educators indicate that suspension of students for disciplinary reasons should be carefully administered to avoid adverse results. Traditional suspension from school for a specified number of days merely adds to the number of potential vandals on the streets and intensifies hostilities. On the other hand, if a suspended student is kept on the grounds and channeled into constructive activities, further alienation is not likely to occur.

Deterrence through Physical Security

Most security programs that rely exclusively on physical security face uphill battles for funds as money for security is diverted from classroom expenditures. Working within budgetary limitations, however, effective strategies can be developed. The following are basic components of a system relying on physical security devices.

1. The necessary initial step in combatting equipment theft, property destruction, arson and certain violent crimes, is to keep unauthorized persons out of the building. Once in the building, damage can be done quickly and the vandal can escape long before response to an alarm is effected.

2. A second step in the physical security approach is use of intrusion alarms, placed at point of entry and in all high loss areas. These alarms fall into the standard categories available for use in any business. Almost every school in the country, however, has a built in advantage for alarms -- the public address system. The p.a. can be modified for audio surveillance at any school when not in session.

3. If a vandal or thief succeeds in penetrating the school undetected, security measures must make it difficult for the thief or vandal to actually steal or vandalize. There are several precautions that should be present in school policies as a matter of course.

- All conceivably portable equipment should be bolted down, if not removed from sight.
- High value items should be removed from sight and kept in locked storage units.
- Equipment should be marked with identification serial numbers to deter fencing, aid in apprehension and facilitate return of stolen items.
- Strict equipment and supply inventory control procedures should be implemented to improve accountability.

- o Vulnerable areas -- libraries, for example -- should be doubly protected, through gates, locked doors.

- o If custodial shifts are employed, they should be staggered to ensure round-the-clock presence in the school facility.

4. The most widely used measure to deter entry is vandal resistant glass. Not only are glass breakage replacement costs saved, but how importantly, access to the building is prevented, illustrating the substantial value of the glass.

5. The employment of silent and local alarms is dependent on the philosophy of the security: local alarms (scare-aways) are beneficial to prevent the theft but rarely result in apprehension; silent alert police or another central station and are most effective for apprehension, rather than prevention.

Arson and damage due to diversionary fires can be greatly minimized through application of alarm systems detecting unauthorized access. Technology provides precautions that do not deter the arsonists, but do succeed in minimizing the damage. Smoke sensors and sprinkler systems should be standard preventive devices. Flame retardant materials are available and should be used whenever possible, in auditorium stage curtains, for example. New schools should be designed to minimize danger of fire spread. The best deterrent, however, is to prevent the would-be arsonist from gaining access to the building.

An example of a school district that has developed a comprehensive physical security program is included in the case studies, in Section II.

Summary

Schools are handicapped to a more significant degree in trying to reduce the $600 million loss to crime than are other sectors. Although professional theft is deterrable, a public school is probably the most visible, symbolic institution in society and it often is destroyed by juveniles disenchanted with that society.

It is readily apparent that within budgetary limitations, a successful security program can be developed. The two extremes in security detailed here -- are complementary, in that a problem solving approach does not deter the $1500 loss of equipment resulting from a professional burglary, and the physical security device does not stop a student from throwing a cherry bomb. Moreover, they are analogous to a traditional business approach to crime prevention: combination of employee (student, teacher) control, management (educator) awareness and perimeter protection.

The contents of schools -- both people and property -- are indispensable and irreplaceable. There are easily applied and workable methods available to ensure the safety of -- and safety in -- the schools. Common sense loss prevention in the nation's schools is needed if losses are to be stemmed and decreased.

Sources:

1. National Association of School Security Directors
1320 S.W. Fourth Street
Fort Lauderdale, Florida 33312
Joseph I. Grealy, President

2. School Product News
Industrial Publishing Company
614 Superior Avenue West
Cleveland, Ohio 44113
(School Security Survey is published annually in a summer edition of this monthly publication)

3. National Education Association of the U.S.
1201 16th Street
Washington, D.C. 20036

4. "Our Nation's Schools -- A Report Card: "A" in School Violence and Vandalism." A preliminary report of the Committee on the Judiciary, Subcommittee to Investigate Juvenile Delinquency, U.S. Senate. (The Subcommittee conducted extensive hearings into educational crime; the report is a summary of the testimony and independent staff research).

CASE STUDY: SCHOOL SYSTEM COMBINES PHYSICAL SECURITY WITH CRIME DETERRENCE ELEMENTS TO ACHIEVE SHARP REDUCTION IN LOSSES

Background: This case study concerns the crime prevention program implemented by a school district located in a large metropolitan area encompassing rural, urban and suburban geographical concentrations. The school system is comprised of 25 facilities: 1 senior high, 2 high, 3 middle, and 19 grammar schools. Total enrollment is 175,000. One senior high services all twelfth grades.

Problem: The school system was experiencing escalating dollar losses due to property crime; also, theft of equipment, destruction of facilities, and locker thefts were major problems. Person-to-person crimes such as extortion, assault, and more violent incidents existed but the frequency was such that these crimes were not identified as a major problem area.

Factors conducive to crime were abundant in the city's schools. Some schools suffered from location in high crime areas of the city; others were likely targets because they served as a repository of high value equipment used as teaching aids. Pressures generated by a mixture of students created the potential for increased student crime, as evidenced by vandalism and locker thefts.

Objective: The school district authorities aimed at developing a cost-effective preventive security program focused on minimizing property losses without disturbing the educational interrelationships among the facility itself, administrators, teachers and students.

Steps Taken: Physical security devices were used to deter crime, although the mere presence of physical security did not, in and of itself, deter crime. Rather, maximum use was made of a systematic approach toward crime prevention involving the following sequence of actions:

(1) measuring losses, to analyze trends and define problems; and

(2) designing and implementing the preventive measures based on risk/cost/benefit analysis.

Loss Measurement, Trend Analysis, and Problem Definition

The initial step taken by the school district toward developing an effective loss reduction program was a crime loss survey to pinpoint specific vulnerabilities and dollar losses incurred by each facility. Losses to vandalism, theft and burglary in the school year 1970-71 were $174,000. Locker thefts increased this figure to approximately $250,000.

The reliability of the survey data was enhanced by standardizing the definitions of crime loss categories. Each official responding to a survey was encouraged to be consistent in providing data in pre-determined categories -- specifying when arson is vandalism, or when vandalism is a burglary, for example.

Since the initial survey, data has been collected and analyzed annually to measure the effectiveness of existing security and to isolate new areas in need of additional attention.

Analysis of the results of the original survey indicated that the primary recurring problem was theft of school property rather than vandalism or person-to-person crimes. The primary criminal being dealt with was the professional thief -- not the juvenile delinquent responsible for losses in many school districts. Thievery was believed to be perpetuated by fencing, which thrived due to the proximity of the metropolitan area. More resources were thus allocated to the major problem -- property crime -- and the potential of the physical system was more highly developed, as a result.

Design and Implementation of Security

This school system obtained Federal funding through the Law Enforcement Assistance Administration's State grant program to finance a comprehensive, integrated crime prevention system.

In 1972, the first year of implementation, the school district obtained $50,000 in Federal funds. In 1973, $30,000 was obtained. Twenty-five thousand dollars and $17,000 were added for 1972 and 1973, respectively, in city funds, resulting in total operating budgets of $75,000 and $47,000.

Whether another school system could implement an identical system of protection without external funding depends on the priorities -- improving security or building new classrooms -- of individual school districts. It is clear, however, that the program designers have implemented a program based on fundamental elements of loss prevention that are applicable in various degrees to any school district.

Policy decisions behind security measures implemented in this school district reflect careful analysis of risks, assets and crime prevention costs; the security measures were installed with regard to individual needs of school facilities. An additional consideration was the requirement that security not impose on, or restrict in any fashion, attainment of educational objectives.

The physical security system that was designed centered on effective use of public address systems, supplemented by alarms and closed circuit television.

A. Public Address System

The 2-way public address (p.a.) already present in each school, was made the basis of the system. The geographical layout of the school system resembled a circle; the p.a. system in each facility was connected via leased telephone to a central station, located roughly in the center of the circle, where the noise was filtered through a "sound analyzer." Burglar or vandal type noises alerted the monitoring officer in the central station to potential trouble. Like many industrial firms, the school system found that a commercial central station was inadequate for security needs, and established an internal station monitored by security officers from 4 p.m. to 8 a.m. on school days, and 24 hours a day on weekends and holidays.

An agreement with the city's police department was formulated to directly tie the central station to police headquarters, through a "hot line," which enabled efficient and quick response to incidents triggered by the system's detection capability.

B. Alarms

The noise detection system was supplemented by various types of alarms, including microwave, infra-red and ultra-sonic. These devices were installed initially in locations in which cost/benefit analysis indicated feasibility. For example, alarms were placed in high value storage, audio-visual, library, business and photographic lab areas. As the school district expanded its facilities and increased its stock of teaching aids and other equipment, the cost/benefit method was employed to ascertain the feasibility of new protection requirements, which were identified by annual loss surveys.

The majority of the alarms installed were local rather than silent in order to prevent the loss by deterring the would-be-thief. When triggered, these alarms emit a jolting noise that frightens and deters the thief. The p.a./sound analyzer system also transmits the alarm sound to the central station -- which sets the security force and police department in motion.

The decision to install "scare-away" devices was predicated on the objective to implement a cost-effective security program. Although apprehension and prosecution of suspects are integral elements to crime reduction, the deterrent concept was believed to result in even greater savings to the system -- obviously if the loss was prevented, there was no suspect to apprehend, no costs incurred in prosecution, no damage to the facility, and no damage to property or loss of equipment that was stolen before apprehension off the premises.

Moreover, the designers perceived that in at least one respect, education was not dissimilar from profit producing enterprises -- costs had to be reduced if the system was to operate efficiently. The impact of budget problems made it increasingly difficult to replace stolen equipment -- especially if the equipment was purchased with state or Federal vocational funds. Then, as now, a two year delay before replacement was routine. Budgetary considerations thus made it imperative to scare the thief away.

C. Closed Circuit Television

To protect the senior high -- the school most vulnerable to crime loss -- closed circuit television was utilized. Although minor complaints were received from parents who found "surveillance" of their children disquieting, implementation of this effective crime prevention tool did not create significant resistance from students.

The cameras were placed in hallways and individual rooms to monitor high value equipment, high volume traffic, and isolated areas. To deter theft of the cameras themselves, each was encased in a custom made steel and thick plastic case.

Results

Many benefits accrue to this school district from the systematic application of its loss prevention program. The most direct result was the dramatic reduction in dollar losses from $250,000 in 1971 to $19,500 in 1975.

Another barometer of the success of this program is provided by the reduction in police utilization. In 1970, police responded to 700 calls; in 1975, only 55 calls were made. At $1,000 per police response to an incident, significant savings to the community obviously have been realized.

Other benefits include the retention of teaching aids, and consequently, an improved educational environment. The program -- through its noise detection and alarm system -- prevents theft of equipment that is irreplaceable in the immediate term.

The effectiveness of the detection system diminishes the likelihood of actual disruption of school; for example, a massive destruction by malicious vandalism is less likely to occur. Moreover, by preventing losses, the system allows a maximum of school funds to be channeled into classrooms -- rather than into continual replacement of stolen items and repair of damaged facilities.

CHAPTER 3

FINANCIAL SERVICES

There are approximately 88,000 financial depository institutions and branches in the U.S. Almost 80 percent are commercial banks and credit unions, with the remainder predominantly savings and loan associations. A very minor portion consists of the fourth type of depository institution, mutual savings banks.

The expansion of time deposits, demand deposits, and assets in the banking system during the past 15 years has resulted in several basic changes necessary to accommodate the expansion. For example, the American Bankers Association estimated that there are 100 million checking accounts at commercial banks. Ninety percent of business is conducted by the exchange of more than 26 billion checks annually. The check volume grows at a 7 percent rate, on an annual basis.

With the "age of consumerism" during the 1960's, banks expanded consumer loan operations, home mortgage loan activity, and credit services, and emphasized retail banking. As the system became consumer-oriented, design of banking offices themselves evolved to accommodate the customer. That means the structure itself lost much of its imposing appearance, in search of a friendly, open, relaxed, and customer-attracting atmosphere. Customer attraction often means visible tellers, addition of lounge areas, removal of caging and metal, display areas and other distractions that make it easier for the criminal to strike without attracting attention.

Banking growth has also resulted in a highly automated system, both for internal and customer usage. According to a 1972 survey conducted by the American Bankers Association and the Bank Administration Institute, 56 percent of all commercial banks used computer facilities. That percentage has grown and automation has expanded to include computer services such as automated tellers and cash dispensing machines -- for customer use.

Simultaneously, the use of bank credit cards has dramatically increased. In 1974, an estimated 70 million Americans used bank cards to obtain $13.8 billion in merchandise and cash advances. These cards are accepted at more than two million retail businesses, with the average purchase about $20.

These growth associated factors combine to create an atmosphere more conducive to crime loss than is present in any other industry. The fuel is, of course, the money, securities, travelers checks and other liquid assets. The igniting element is the lack of proper management controls that are designed to avoid the explosion -- the robbery, burglary or embezzlement.

Dollar Losses and Incidents

Tables VI and VII reflect the losses to federally insured depository institutions, both in dollars and number of incidents.

The Federal Bureau of Investigation reports that fraud and embezzlement, in federally insured banks, rose in fiscal year 1976, while robberies, burglaries and larcencies declined. Bank fraud and embezzlement violations have risen sevenfold in the last decade alone. The net loss from bank fraud and embezzlement rose 14 percent to $175.8 million in FY 1976 over $154.8 million in FY 1975. Actual incidents rose 8 percent from 10,181 in FY 1975 to 11,071 in FY 1976.

TABLE VI

Burglary, Robbery, Larceny Incidents and Losses by Type of Depository Institution, FY 1976[1]

	Commercial	Mutual Savings Banks	Savings & Loans	Credit Unions
Burglary Incidents	240	4	35	71
Robbery Incidents	2,732	143	885	54
Larceny Incidents	307	4	27	9
TOTAL FOR FOUR CATEGORIES:				
Incidents		4,511		
Losses (millions)[2]		$27.3		
Net Losses[3]		$22.3		

[1] Source: Federal Bureau of Investigation

[2] Loss data are available only in aggregate

[3] Net Losses = Total - Recovery

TABLE VII

Bank Fraud and Embezzlement Incidents and Losses, by Type of Depository Institution, FY 1976[1]

	Commercial	Mutual Savings Savings & Loans	Credit Unions	Total
Incidents	9,365	824	612	11,071
Losses (Millions)	$185.3	$17.9	$3.1	$206.3
Net Losses[2]				$175.8

[1] Source: Federal Bureau of Investigation

[2] Net Loss = Total Loss - Recovery

Fraud and embezzlement are invisible crimes -- the ones frequently not reported out of fear that publicity would be harmful to a bank's reputation. The annual upsurge in the FBI bank fraud and embezzlement statistics, which are based only on reported offenses, reflects more than merely large increases in criminal activity. More significantly, the percentage increase indicates an erosion of banker's traditional resistance to prosecution of embezzlers and swindlers. This increase has occurred due to an increasing sensitivity to the economic impact of crime which outweighs the consequences of adverse publicity. Reporting habits have improved also due to the guidelines established by the Comptroller of the Currency, which require embezzlements to be reported to the FBI, the U.S. Attorney, bonding company and the regional administrator. Any embezzlement or unexplained shortage of $1000 or more is subject to the reporting requirements. Reporting procedures, however, still retain room for improvement; financial institutions are no exception to the general rule in industry that the reported crime is only the tip of the iceberg.

Although causes will be dealt with in more detail in the section on vulnerabilities, it is apparent that improved reporting is not solely responsible for the large annual increase in embezzlement and fraud. A recessionary economy, coupled with inflation, increases the attractiveness of this type of crime as an easy cash source for both employees and non-employees otherwise unable to meet financial obligations.

While embezzlements and frauds increased, robberies, burglaries and larcenies (Table VI) dropped 10 percent in FY 1976 from a record high in FY 1975. Losses reached $29.3 million. Cases involving kidnapping of hostages and threats against personal or corporate property fell 23 percent from 373 in 1975 to 286 in 1976.

Bank robberies and burglaries have risen 400 percent over the last decade. Industry sources cite many reasons for the increase in addition to standard explanations. These include the proliferation of branches in areas convenient to depositors -- near major transportation arteries, for example. These areas also provide convenient get-away routes for criminals. Another factor that impacts is the extension of business hours -- again, for customer convenience. Many banks extend hours into darkness, an innovation which provides better cover to the criminal than does broad daylight. The major factor contributing to the increase, however, was the failure of banks to provide adequate security measures. The drop in these crimes in FY 1976 indicates that the industry has begun to progress in this critical area.

The drop in robberies and burglaries also should be viewed in light of the Bank Protection Act of 1968, which induced major bank regulatory agencies (Federal Deposit Insurance Corporation, Federal Reserve System, Comptroller of the Currency) to implement stricter regulations providing for mandatory bank security. The regulations require, for example, that each bank designate a security officer with responsibility for determining the protection needs of an individual bank, and require a program of security instruction be provided to employees on (1) employee responsibility (2) security device use and (3) robbery procedures.

Newer, more sophisticated deterrents, such as video-tape cameras, are also responsible for the drop. Some banks have abandoned the customer oriented atmosphere and deal with customers via pneumatic tubes and videotape, or through bullet resistant glass with microphones. Many banks opt for counter to ceiling acrylic protection. A plethora of devices are available to bank management that aid in suspect apprehension -- including trick money and exploding dye packets.

The use of extra-sensitive alarms is prevalent and is another factor that accounts for a decline in robbery and burglary, especially the latter. The general consensus of industry experts regarding violent crimes is that burglary is a negligible problem and that robbery is the primary threat.

Vulnerabilities

The lure of money motivates a wide range of plans designed to rob, embezzle and defraud banks. A comparison of the figures, however, reveals clearly that the major threat to a financial institution is embezzlement and fraud. In commercial banks and credit unions, non-violent crimes occur three times as frequently as violent crimes such as robbery and burglary. According to the FBI figures in Tables VI and VII, depository institutions lose 8 times the amount of money -- $175.8 million -- to employees and swindlers that they do to street criminals. Because of this disparity between non-violent and violent crimes and also because bank robbery prevention techniques are better derived from experts, the remainder of this section centers on the non-violent crimes of embezzlement and fraud.

Within the broad category of embezzlement, certain major risks are identifiable. The internal automation of a bank eases the way for embezzlers and has become by far the most sensitive risk.

For example, employees can juggle accounts to cover up their embezzlement by debiting and crediting selected accounts. This type of automated crime, as is most, is aided by a failure of bank depositors (usually large commercial accounts) to alert bank officials to deviant activity reflected on monthly statements, and a corresponding failure of bank officials to follow up on the leads provided by those who do complain.

Employees also embezzle by tapping dormant accounts. Bank employees, in the absence of proper controls, spot dormant accounts -- those with sizable sums of money that are not used, usually belonging to older clients.

Security-conscious bank managers perceive the inherent risk in dormant accounts and establish separate controls to minimize it. Control can be computerized to have sudden activity in a dormant account trigger an exception, or it can be as simple as requiring dual approval over withdrawals.

Still another method employees use is embezzling the fractions of interest on depositors savings accounts. Many savings and loan associations compute interest daily that builds up additional small fractional amounts on an account. In at least one instance, a bank employee programmed the computer to send all the resulting fractions of cents to his account -- $17,000 was embezzled in four years.

Automation makes unlikely crimes possible: one bank was defrauded of several thousands of dollars when a depositor substituted his coded deposited slips for the blanks in the bank's lobby. All deposits were subsequently credited to his account. The section on computer abuse (page 106) addresses in more detail the impact of this crime.

A second major risk area in embezzlement are bank officers, and other long term, trusted employees. The FBI attributes the major portion of fraud and embezzlement losses -- at least during the last five years -- to highly placed officers and directors of the victimized institutions.

Loan officers, if not working within a closely controlled environment, have optimum opportunity to defraud their bank. Fraudulent approval of legitimate or fictitious loans, can be extraordinarily easy for the loan officer. Highly placed officers can be bribed to approve loans for marginal companies. Loan officers who are connected with other businesses in a directorship position, for example, can easily arrange loans to those companies, if the business is not otherwise qualified. Loan officers can also embezzle be merely approving fictitious loans.

The third and most severe risk is the lack or the laxity of operating controls. In one well-known instance, an employee -- a vault teller -- stole $168,000 in a brown bag by carrying it through the exit guarded by a security officer, whose duties included package inspection. He told the guard that it was a pet rabbit. It was a failure of an established control that caused this loss.

There have been reported instances of employees "borrowing" cash on their lunch hours for betting purposes -- hoping to win enough on the bet to make a profit after return of the original money. The bank loses when the employee has an unlucky day; the loss is a frequent example of the risk faced when bank managers do not enforce basic operating procedures.

Internal fraud, as distinguished from embezzlement, can be perpetrated either by employees acting alone or by employees in collusion with outsiders. When collusion is involved, crimes become ingenious and thus difficult to counter. It is normally the insider's access to documentation material within a bank that makes that employee invaluable to an outsider. For example, an employee selects a target account. Then a signature card switch is arranged, although the outsider can also perfect a forgery on the original card. The checks are drawn. Such a scheme can result in a windfall before detection -- which hopefully would occur when the account holder receives a monthly statement. Loan officers are also a prime source for outsiders to tap for collusion partners.

The most prevalent externally perpetrated fraud is the check swindle, usually done by forgery of stolen checks. The American Bankers Association advises banks to extend "full service" banking cautiously, as the risks often outweigh the competitive benefits. This advice stems from an estimated $50 million loss to banks from forged checks passed by non-employees who are usually able to con the employee into trusting the legitimacy of their identity.

Increasing use of false identification by check swindlers intensifies the problem. Bank personnel are similar to personnel in most industries: there is no assured method of the validating identification. The report of the Federal Advisory Committee on False Identification, Department of Justice, estimates that false ID's cost business in excess of $1 billion annually.

Crime Prevention

All of the above vulnerabilities are created through management's nonrecognition of crime deterrence as an essential facet of operating procedures. The presence of money -- cold cash -- in the financial institution attracts crime and motivates ingenious plans to steal the money. The extent and varieties of embezzlement and fraud induce industry experts to stress the necessity of internal management controls. Experts participating in the California seminars[1] agreed that such controls should follow a reasonable approach to bank security; that is, they should force a manager to look at operations from a standpoint of logic. There are many relatively minor policies -- in terms of cost and ease of implementation -- that combine to deprive potential embezzlers and swindlers of opportunities.

For example, a successful embezzlement takes time. The bank manager should not give bank employees that valuable time. Duties should be rotated, mandatory vacations established, and overtime strictly supervised. Employees who balk at such controls have a reason for their reluctance; too often, that reason is embezzlement. Management must be sensitive, therefore, to employees' reaction to such policies. The employee who is never ill, or comes to work despite illness, might also have an ulterior motive not founded in loyalty to the bank.

An embezzlement can also be successful because of the lack of frequent reviews designed to catch errors, both intentional and innocent. These reviews should resemble a system of checks and balances -- for example, dual controls over physical handling or custody of vault cash, travelers' cheques, and securities.

[1] "Crimes Against Business: A Management Perspective" Proceedings of Seminars Held in San Francisco and Los Angeles, February, 1976. See Section on Embezzlement.

Some major banks conduct daily reviews, with full scale auditing done on a yearly basis, in addition to certifications and surprise verifications.

These reviews should enforce more basic controls. The control of dormant accounts is a necessity. Similarly, loan officers must not work unsupervised. Frequent reviews of loan approvals should be conducted. An adjunct to loan officer control is careful examination of outside business affiliations.

An often successful technique to detect problems at an early stage is to follow up on customers' complaints. For example, an embezzlement through account juggling can be detected should a depositor alert the bank to a statement which shows unwarranted activity. The value of such external aids is lost if the complaint is not investigated. Moreover, when a depositor complains to an officer, that officer should not refer the depositor to the employee who originally handled the matter. That employee -- if an embezzler -- rectifies the complaint by tapping someone else's account.

Managers should always be sensitive to personnel problems. The sensitivity must exist before the employee is hired and extend through the employee's departure. Several areas in the pre-screening employment phase warrant attention. Extra precaution must be given when employing a person with chronic financial problems; for this reason, bank personnel officers should obtain credit reports on applicants -- within the guidelines of the Fair Credit Reporting Act. (See further discussion on page 98). Applicants afflicted with active alcoholism, drug, gambling or betting problems, are not always the best prospects for jobs requiring money-handling. Other personal problems or lifestyles are important considerations in the employment phase -- can the prospective employee meet his financial obligations on the offered salary, for example.

A particular problem is presented with the "floater." Although the "floater" problem exists in most service industries, the impact is greater in the financial services sector. Banks have traditionally avoided prosecution of embezzlers to circumvent adverse publicity; the embezzler often "resigns" in return for a letter of recommendation, which clears the way for the employee to victimize another bank. The increasing reporting of embezzlements and swindlers tends to ameliorate the floater problem since after prosecution the information becomes a matter of public record. For a fuller discussion of privacy legislation, see page 107.

Other pre-screening guidelines, listed on page 101, should not be circumvented. Once the applicant has participated in training and orientation sessions, management's attention to personal details should not decline.

Industry sources cite disparate salary levels as a frequent cause of embezzlement. For example, a veteran employee of 40 years service resents receiving a salary barely more than a management trainee. Not only can disparate salary levels give rise to dishonesty, but also generally low pay can be responsible. One Memphis bank, severely victimized by corruption, partially rectified temptations to embezzlement by giving across-the-board pay increases. Although the pay increase was not the only implemented correction, the bank was able to cut losses significantly.

Lifestyle of an employee can be a good clue. If a change in type and amount of expenditures occurs that is not induced by a promotion or is out of proportion to promotion, it can be indicative of external sources of income. Because there are a variety of sources -- many legitimate -- for the extra income, a supervisor's sensitivity must separate the valid from the invalid. Tip-offs can occur if expensive vacations are taken by a lower salaried employee or if a lower salaried employee buys a Cadillac or Mercedes, for example.

In addition to managerial initiated controls -- supervision, operations, pre-employment screening -- managers should also be aware of the benefits automation bestows on a security policy. The increasing prevalence of automation enables the development of exception reporting and trend analysis for the use of the auditing department. Auditors can be detailed to an individual office should the number or type of exceptions warrant it.

Summary

Bank managers formulating a crime proof system are faced with pressures more intense than in any other sector, generated by the vast temptation of money and the basic human quality of the crime. The crime-proof system is only possible if designed with checks and balances that ferret out the unusual -- from the expensive car to the complaining depositor to the exceptions report. Ultimately, the success of any individual system depends on the after-the-fact cooperation with law enforcement and the banks willingness to prosecute -- not only the armed robbers but the long time, trusted officer.

CHAPTER 4

HEALTH CARE SERVICES

Hospitals are the major segment within the health care service sector. The costs of hospital care, for which consumers spent an estimated $56 billion in 1976, have been rising, forcing both public and industry examination into the causes of rising costs.

Most frequently cited as contributing factors to rising costs are decreasing occupancy levels, and increasing expenses such as wages, equipment and utilities as well as an expansion in services due to an expansion in technology.

It is rapidly becoming apparent that crime losses -- primarily from theft and other business related crime -- are partially responsible for the upward trends in costs of health care. Also contributing to the cost of crime is the cost of preventing it. Many reasons explain the problem within the sector.

Most traditional, and least problem solving oriented, is that a hospital is merely a microcosm of the community which it serves and consequently cannot avoid the crime. A similar rationale, equally as traditional, explains crime against hospitals as societal unrest, inasmuch as hospitals are to some symbols of society.

The most compelling reason for increased vulnerability to crime, however, is the attractiveness of a vastly expanded inventory, combined with larger facilities and staffs, which make effective controls difficult to formulate and enforce, and which make the hospital an inviting target for crime. Hospitals are now "big business" -- there is much to steal and many persons to prey upon.

Expansion has been stimulated by increased demand for health care services resulting from both the national health programs and new medical knowledge and capabilities induced by rapidly advancing medical technology. Increasing consumer awareness of the advancements has contributed significantly to expansion. The diversification of hospital services compounds the risk of loss by multiplying the operating layers, personnel and inventory necessary to run a hospital.

A corresponding factor in crime is the mere magnitude of persons that hospitals deal with on a daily basis. On any given day, there are at least 1.2 million patients in hospitals, 600,000 patients utilizing out-patient facilities, and 164,000 persons receiving treatment in emergency rooms. When visitors, professional, and support staff to these million plus patients are included, the exposure of the hospital facility to potential crime is phenomenal.

Dollar Losses

Estimates of dollar losses in hospitals attributable to crime vary. One industry source cites loss equivalent to $1000 per bed annually. There are however, no estimates documented by a sound statistical base. Certain industry executives agree that 3 percent of any operating budget is a fairly accurate measure of crime loss. A more accurate estimate of exact losses incurred by health care facilities suffers a problem similar to other industries in that a large number of losses go unreported. Some industry representatives indicate that this problem is much more acute in hospitals than in other settings.

Although accurate record keeping would provide more adequate loss data, the infinite risks to crime experienced by a typical hospital can make record keeping burdensome. For example, potential crimes against patients and employees include: murder, rape, robbery, assault, burglary, larceny, or kidnapping. Some of the most notorious crimes in hospitals are those involving kidnapping of new born infants from nurseries and those involving murder of patients through poisonous injections. Such cases usually involve trespassers posing as hospital employees.

An additional stumbling block to assessing risks concerns patient's property. Patients frequently bring money or property to the hospital for the duration of their stay. Although most hospitals maintain a valuables check-in system for such patients, the patients often don't use the system, and consequently expose their property to theft.

Theft of patients' property presents a sensitive, difficult problem to hospital administrators. In most states, hospitals are not legally bound to replace, or reimburse patients, for property lost or stolen from a patients while under the care of the hospital. According to industry estimates, the actual dollar value of patients' property thefts are very small when compared to inventory shrinkage due to theft, and the potential damage to good community relations prompts some hospital administrators to reimburse victimized patients', regardless of legal immunity.

The factor that complicates the patients' property problem is the determination of actual loss to the patients. It is not unusual for property reported stolen by the patient to be non-existent, safely at home, misplaced in the patients room or borrowed by another patient.

Hospital employees, particularly the nursing staffs, which are predominantly female, are vulnerable to assault or rape. This vulnerability increases on night shifts, as isolation is greater; the majority of hospitals are cognizant of the risk to the staff during night shifts and shift changes and most provide night escort and patrol security. Hospital security routinely extends to student residence of training schools incorporated into the hospital; especially since the 1968 incident in a student dormitory on hospital premises that resulted in the death of eight student nurses.

Although by necessity concerned with the potential for violent crime, and the corresponding urgency to develop deterrents to this potential, hospital administrators are becoming more aware of the severity of losses resulting from theft of the assets of the hospital. Non-violent, "business" crime causes the majority of the typical hospital's costs of crime; these will be dealt with here.

Vulnerabilities

A hospital's vulnerability is created by its inventory, which is even more attractive to crime than, for example, the inventory of a lodging facility. Linen, food, drugs, medical equipment, and personal items comprise the bulk of the inventory. The vulnerability to business crime is compounded by the potential for embezzlement and computer abuse.

An extraordinary high number of hospital inventory items are easily sold on outside markets and are in demand for personal consumption. These characteristics apply in particular to medical equipment, supplies, drug and linen inventory.

Product technology has contributed significantly to the theft of medical equipment items by making them easier to steal. The large percentage of medical inventory items are lightweight, disposable, and compact. For example, wheel chairs were stolen rarely, if at all, until the collapsible, lightweight model became the standard wheel chair in use. Another example is disposable syringes.

Inventory items -- especially those used for patient care -- become more susceptible to potential theft through lack of adequate inventory control measures and the open availability of the product in supply centers.

A second inventory staple attractive to thieves is linen. Apparently, the volume of linen used in an average hospital, combined with the exposure it receives, are factors responsible for crime vulnerability. For example, a large hospital can use 17,000 washcloths a month -- and the addition of gowns, sheets, surgical wear, diapers, and towels to the supply is an invitation to crime, particularly since linen can be readily used.

The other predominant factor contributing to linen losses is the prolonged exposure of linen during the laundry-to-storage-to-usage cycle. The thief does not differentiate between soiled and clean or used and new linen supplies.

A third inventory item susceptible to loss are drugs. Scheduled narcotics are susceptible to employee and other non-violent theft; employees either pilfer small quantities or obtain the narcotics through false prescriptions, in the absence of adequate controls. Industry sources hold employees accountable for the majority of narcotic losses.

Hospitals are primary targets for drug motivated crimes and thus drug inventories carry special risks. The drug inventory is one of the few consistent targets for armed robbers and burglars, primarily because it is an obvious source of schedule narcotics. Most hospitals recognize the potential danger of armed intrusion and thus protect the pharmacy with alarms, CCTV and increased personnel.

The maintenance of narcotics is strictly regulated by the Controlled Substance Act of 1971 and is enforced by the Drug Enforcement Administration. The potential for crime exists despite compliance with these Federal regulations.

Employee Theft

The majority of these inventory losses are caused by employee theft. A typical hospital is responsible for specialized services requiring as many as 145 different job skills. Professional staff nurses, doctors, and administrators, comprise over fifty percent of the staff. In some non-professional jobs annual turnover exceeds 50 percent. Many low skilled health care workers are transient and float from hospital to hospital. This diversity and transiency of the staff makes effective controls difficult to design, much less enforce.

Employee theft in hospitals is perpetrated by both professional and non-professional staff. For example, the medical staff is supplied with stethoscopes, microscopes, blood pressure testers, and similar equipment for use in hospital practice only. A large percentage accompany the doctor into private practice and represent a significant cause of inventory shrinkage to the hospital.

Crime Prevention

Faced with escalating losses, incurred primarily through employee theft, one of the most pressing needs in hospitals today is development of crime deterrent policies that reduce opportunity for theft and tighten control over inventory. A corresponding urgency, although not within the scope of this report, is the development of employee and patient safety programs.

The initial step must be development of comprehensive record keeping. Fundamental to any loss prevention program, it means not only data collecting, but analysis and trend distinguishment to answer integral questions such as how much, where, how and when are losses incurred. Record keeping, moreover, is an invaluable aid when budgetary programs are presented to hospital boards, and is highlighted in the accompanying case study.

Pre-employment screening is essential in a health care facility, because the majority of crime losses can be attributed to employee theft. Special care must be taken to avoid hiring the "floating" hospital worker.

Although hiring controls are difficult to establish and only minimal control can be exerted over the medical staffs, controls can and should be established over the non-professional staff, and should exceed routine fingerprinting and arrest record check, to include comprehensive pre-employment screening as outlined in the section on personnel. Moreover, liaison among personnel, security, and medical staff heads can provide a stabilizing factor by alerting security to personnel problems in both professional and non-professional areas.

After hiring, employee controls should continue and participatory management exercised, again as outlined in the section on personnel security.

Employee orientation should extend to the entire staff, to acquaint them with the security program. Training programs should stress proper usage of supplies, especially linen, to avoid loss through waste or negligence.

The most critical portion of a hospital's security program must be inventory control. A system should be established that enables detection of irregulatities in inventory usage with minimum impediments. This can be done by imputing usage medians; that is, given the number of beds, rate of occupancy, type of care provided, a usage schedule for most items can be computed.

On a regular basis, actual usage figures should be reviewed in comparison to the median usage schedules. If actual usage is abnormally high, the discrepancy should be investigated.

A supplementary control can use existing hospital procedures. Normally, the re-order of medical equipment must be justified although supplies are exempt from the procedure. Effective early warning of a problem could be gained through requiring all re-orders of inventory to be justified and requiring them to be channeled through security. A variation, less burdensome, would route invoices through security. Both these methods provide reliable insight into inventory activity. Depending on the item, frequent re-ordering can often signal inventory shrinkage. Discrepancies should be investigated.

Most experts in the field further stress key controls as a basic method to secure inventories. The primary concern is the maximum possible reduction in the number and distribution of keys to storage units. This again reduces the risk by reducing opportunity and exposure.

The interplay between reliable personnel and inventory control is obvious. If line management responsible for control over records are themselves the thiefs or are indifferent, negating controls becomes a matter of ingenuity and time. Thus, actual inventory auditing is mandatory to prevent such schemes. Auditing should be done on an irregular basis -- so as not to give advance warning.

Hospitals, especially those with expansive, multi-building facilities, can also give consideration to developing an access control procedure which would reduce the exposure of the assets.

One view toward access control is the issuance of photo identification badges color coded to relay immediately the employee's exact duty station. If required to be displayed, badges have two immediately apparent uses: (1) to enable hospital officials to immediately differentiate between employees and outsiders and (2) to enable supervisors to account for authorized staff in the unit. Many experts do not advocate the use of ID badges, for a variety of reasons. Many cite their cost ineffectiveness, and their inapplicability in a fluid setting.

Another view of access control holds that visitors check in at the minimum, and, ideally, register and receive passes. The burden of this control can be great, especially in larger sized facilities. Yet, if this aspect of crime control is completely ignored, a hospital can invite losses incurred by a nonchalant trespasser.

Non-hospital affiliated persons are responsible for a relatively small amount of total losses. The kernel of the external loss problem lies with persons gaining legitimate entry to the hospital through false pretenses. For example, criminals can enter as visitors, maintenance, service, personnel, as well as laboratory technicians and other professional medical staff. Access control -- in some form -- is essential to a reasonably effective security program.

Summary

In many respects, crime prevention in hospitals is similar to that in other industries. For example, cost effectiveness, ease of implementation, consistency with established policy and potential benefits are factors that enter into the formulation of a crime policy for the hospital.

But unlike other industry, a hospital crime prevention program must be designed to incorporate unique operating situations. Beside the obvious differences -- 24 hours a day, seven days a week operation, and the steady influx of visitors -- the organizational structure of a hospital complicates security. The hospital administration is subordinate to a Board or similar body, which is not involved in day to day functioning of the facility. Yet budgetary decision making responsibility often lies with this Board.

Crime prevention in hospitals is hampered most seriously by the obligation of these decision-makers to allocate extremely scarce resources to competing areas. The humanitarian purpose for which a hospital exists underlies most decisions. For example, decisions often necessitate choices between medical life saving equipment and security devices which would deter illegal activities, possibly including violence. The conflict that arises can't be avoided and thus is a serious impediment to progressive security.

Despite the increasing losses, and the increasing awareness within the industry, most hospital crime prevention policies are based on "management-by-crisis," consisting entirely of reactions to losses already incurred. This philosophy has developed because of the difficulty in convincing administrators and Board members that security deterrent expenditures are necessary.

Sources:

1. Colling, Russell, *Hospital Security*
   Security World Publishing Co., 1976.

2. International Association for
   Hospital Security

   Northwestern Memorial Hospital
   250 E. Superior Street
   Chicago, Illinois 60611
   Secretary: Keith MacKellar

3. Morse, George P. and Morse, Robert F., *Protection of a Health Care Facility: A Loss Management System for all Industry*, Williams and Wilkins, 1974.

4. McShea, Kelvin M., "Expansion of the Present Concept of Hospital Security: A Managerial Perspective." (Obtain from IAHS, at above address)

CASE STUDY: HOSPITAL ALLOCATES RESOURCES EFFECTIVELY TO MINIMIZE CRIME

Background: A 1,700 bed county hospital located in an outlying suburb of a large midwestern city, this facility is considered an "extended care" facility; patients are admitted only if chronically, not terminally, ill. Many patients are non-ambulatory and are legally classified as non-responsible. The hospital has limited surgical, research and emergency facilities, but has extensive theurapeutic facilities for stroke and muscular patients.

Several separate buildings comprise the sprawling hospital. Composition of the 2,300 member staff of the hospital conforms to the industry average: approximately 50 percent professional and 50 percent support personnel.

Problem: The hospital was experiencing a significant increase in direct and operating efficiency losses from crime. Vulnerabilities facing this particular hospital were employee theft and to a lesser extent external threats. Additional problems resulted from patient involvement in incidents and the mental incapacity of some patients involved.

Access control was not a significant problem -- it was easy enough to distinguish visitors from trespassers in a chronic care facility with its long confinements of patients. However, the more relaxed atmosphere of a long term facility (compared to the often chaotic tempo of short term hospitals) meant that unpredictable incidents would occur, as patients are free to roam at will rather than being restricted to their rooms. Problems were severe enough to warrant more than the "friendly guard" approach.

Objective: To reduce losses through a policy of crime deterrence, emphasizing round-the-clock, multifaceted protection against employee, patient, and external theft. An additional consideration was to fashion security so as not to impose too greatly upon patients -- many of whom had been at the facility for extended periods of time.

Steps Taken: The security program developed in this hospital illustrates a traditional approach emphasizing manpower, as opposed to physical security measures. It is a completely in-house program, with loss measurement, trend analysis, vulnerability assessment, and a general awareness by top management of "what's going on." Specifically, the security program designers concentrated on developing three areas responsible for the program's effectiveness:

(1) the structure of the security department and its relationship to hospital management

(2) a comprehensive record keeping system

(3) use of proper techniques to anticipate and handle the crime

Structure of the Security Department and its Relationship to Hospital Management

The in-house security department was made a separate operating unit within the hospital. Today, it is comprised of a 28 member staff that resembles a mini-police force. Its operating budget approximates $450,000 annually -- which far exceeds security budgets in similar-sized facilities in the same area. The structure and composition of the department very much reflects the industry view that a hospital is a microcosm of the community.

Since the objective of this security program was and continues to be loss reduction and deterrence, the department was structured to achieve a high degree of visibility. All officers are uniformed, radio equipped and patrol the grounds in squad cars or motorcycles. They are not, however, armed. The decisions not to arm but to uniform and equip officers with high-visibility law enforcement symbols were based on the assessment of vulnerabilities and objectives, given the framework within which the security functions.

In addition to security, the department was made responsible for fire prevention and control; its importance is emphasized by the assignment of full-time security personnel to this function. Other responsibilities include Occupational Safety and Health Administration (OSHA) regulations and workers' compensation, but the paperwork for these tasks is handled by full-time clerical personnel -- allowing security officers to devote a higher percentage of their time to strict security functions. The hospital management decided to exclude physical plant maintenance entirely from the department's responsibilities, in order to reinforce the impression that security is security -- not maintenance.

Program divisibility, as implemented and practiced by this hospital, has two direct advantages: it professionalizes security, enhancing its reputation with the staff, and it allows concentration on the primary problem -- reducing crime and its impact. This organizational structure allowed the facility to avoid a handicap many hospital security programs face by being the catch-all department for functions that do not fit anywhere else in the organization. As a result, security in these other facilities is often an incidental task, with other functions intruding and the security department losing its unfettered focus on the security problem.

Since security was implemented as a full-time function of one department in this hospital, its position in the organization ensured access to the administrator and through him to the decision makers of the governing board. This access was enhanced by a high degree of security-consciousness on the part of the individual serving as administrator in this case.

Record Keeping System

The security policy of the hospital was predicated on deterrence and remains anticipatory to crime. The primary element that implements this policy is the record keeping system.

The basic tool now used in this hospital's record keeping system is a security incident form, a relatively standard form usable in any industry. A copy of the report form is on the next page. All incidents requiring utilization of security personnel are reported by the officer involved in the incident.

The designers of the security program perceived three advantages to record keeping which have proven their worth:

(1) Loss measurement made possible trend analysis -- the key to anticipating and deterring crime, thereby preventing the loss. Analyses are used to determine physical security deployment and manpower allocation for anticipatory measures.

An index card system was set up as the focal point for the records to allow for extraction of essential data from the security incident forms. Cross-referencing in the index card system under such subject headings as the officer involved, the victim, the complainant, witnesses, the date, and the security incident number was a major emphasis.

(2) Record keeping can provide hospital boards with the justification needed for security expenditures by pinpointing crime incidence and losses attributable to crime. Without documentation that preventable crime does occur -- i.e., the

SECURITY DEPARTMENT

DATE OF REPORT TIME OF REPORT		FILE NUMBER
1. NATURE OF INCIDENT	2. LOCATION OF INCIDENT	3. OCCURRED: DATE TIME
4. NAME OF COMPLAINANT	5. ADDRESS PHONE	6. HOW ASSIGNMENT RECEIVED: (check one) RADIO □ ON VIEW □ SUPERVISOR □

NARRATIVE: DESCRIBE INCIDENT REPORTED OR DISCOVERED AND ACTION TAKEN. GIVE NAMES AND ADDRESSES OF PERSONS INTERVIEWED AND NAMES OF OTHERS NOTIFIED OF INCIDENT. BE SURE TO GET NAMES AND ADDRESSES OF WITNESSES, LICENSE AND STICKER NUMBER WHEN VEHICLES ARE INVOLVED.

REPORTING OFFICER STAR	REPORTING OFFICER STAR	SUPERVISOR APPROVING RANK

existing security is insufficient -- security is not likely to receive increased funds.

To fulfill the second function of record keeping, systematic compilation of incidents is made; yearly activity reports are the culmination of the record keeping. The reports are used in annual budget processes and are partially responsible for the ability of the security department to maintain its level of funding.

(3) Record keeping allowed a more efficient allocation of security personnel. For example, a more efficient manpower allocation was realized by the determination that the majority of the 7,000 annually filed security incidents are not criminally instigated.

Proper Techniques for Anticipating and Handling Crime Incidents

Many problems that plague hospital security in general were present in this hospital. By anticipating the existence of sensitive issues and providing for them, the hospital continues to reduce losses and increase operating efficiency.

The theft obviously committed by a patient is an illustration of one sensitive recurring problem. Since this hospital has many legally incompetent patients, the problem was identified as significant. For example, a competency exam is administered to all patients suspected of involvement in a crime; those found incompetent are not prosecuted. Moreover, the patient who continually steals is identified by the cross-indexing in the record system. Consequently the hospital conserves the time and monetary expenditures involved in assessing the competency of such patients.

A second, more severe vulnerability to crime losses within this hospital is employee theft -- directed at the property of both the patients and the hospital.

Staff access to patients makes theft of their property a major target area of crime in the hospital. However, the determination of the cause of theft of an item belonging to a patient is complicated in this hospital by the recurring problem that the "stolen" item often never existed, was misplaced, taken home or borrowed unintentionally by another patient. Again, cross-indexing in the record system identifies those patients who have a tendency to report such "thefts," and prolonged investigation of fictitious thefts is avoided.

Staff access to inventory was another target area of employee crime. A policy was formulated whereby all justifications for new equipment and re-orders of supplies are routed through security. Such a policy minimizes the chance that employee pilferage is depleting the inventory.

A major aspect of the hospital's crime deterrent policy is its generally rigid rule of prosecuting the employees and patients who are suspected of involvement in crimes. As noted above, however, incompetent patients are not prosecuted, and most employees are given the option of resigning before being formally charged by law enforcement with the crime.

The complexity and sensitivity involved in the decision to formally proceed against the patient or employee suspected of a crime mandates a thorough investigation. For this reason, investigators employ full-fledged investigatory techniques recommended by the local law enforcement authorities.

Though prosecution is costly and time consuming, this hospital does not allow the expense to rationalize non-prosecution. Instead, management minimizes the cost and time by making informed decisions at the pre-prosecution stage. That is, the staff is fully aware of the evidentiary requirements, which, when fulfilled through standardized evidence-gathering techniques, ensure that the case is accepted by the prosecutor.

The threat of external losses, i.e., burglary and robbery, was identified as a lesser risk by management. Reflecting this, physical security measures have not been extensively developed. Most of the doors to individual buildings are equipped at least with battery powered alarms and the more vulnerable areas within the facility -- such as the bank or pharmacy -- are equipped with more sophisticated devices.

Results

This facility no longer has a significant crime problem. There is a low rate of criminal incidence -- only 15-20 employees/patients are formally charged with crime annually. Over 7,000 security incidents are filed annually but most of these are minor problems and losses are minimal.

The efficiency and effectiveness of the department -- which operates as an integral part of the hospital routine -- is attributable to the consistent application and development of the key security principles outlined above.

CHAPTER 5

LODGING SERVICES

The hotel/motel industry today is essentially a product of post World War II attitudes and life style changes as the mobility of the population has created a wholly different concept of the service. There are over 45,000 commercial lodging establishments to accommodate the needs of an increasingly individualized population. Although chains account for over 40 percent of total rooms, the extensive geographical and customer diversity of the industry makes generalizations usually difficult.

Rapid growth in the industry has given rise to many transitional uncertainties. Many of the problems associated with the growth, moreover, only now are emerging; consequently, viable solutions for many are not yet within grasp.

Crime problems must be included in this category. The economic impact of direct property losses is compounded by the impact of personal crime on customers, since if personal crime is not controlled, it reduces profits by reducing occupancy rates. Although property crime incurs greater losses, personal crime has far greater impact in terms of public relations and legal expenses, and the significance of the crime problem to this sector is illustrated vividly by the major East Coast hotel that advertises nationally "come and stay with us, where you'll be safe."

One aspect of crime keenly felt by the lodging industry is community crime -- as opposed to business crime. Although the issue of violent crime and its impact upon society is not within the scope of this business-oriented publication, industry sources consider it to be of equal concern, especially as community crime rates can affect occupancy rates of hotels and motels. Crime in the nation's cities continues to receive substantial media coverage and as a result, the lodging industry often must combat the image of a "crime-ridden" community before there is even a need to worry about business crime within the facility. Moreover, if customers are afraid to come to the city, occupancy rates and profits decrease rapidly. Many sources within the industry believe that significant progress has been achieved in this area.

Management problems in designing security programs to reduce losses stemming from property and personal crime are typical of difficulties facing many services. The lodging industry markets a service based in large part on image, and hospitality is an important element in establishing the images that will translate into profits. Crime controls can impair the hospitality of a hotel or motel if not carefully structured and implemented; that is, the remedy can be worse than the injury.

The lodging industry has not overcome this problem, and as a result, crime prevention in the lodging industry is fragmentary. Moreover, in at least two major motel/hotel corporations, the decisions for crime prevention are left to the individual operator. Although in this type of arrangement, the corporation usually has a corporate security department, it is only advisory in nature to non-wholly owned facilities. The individual operator has diminished capacity to deal with problems as security deterrence has not been considered a major responsibility.

Current indications are that security is becoming a priority in many areas. In certain major metropolitan areas, for example, local security groups have been organized which have proven effective in reducing crime victimization and losses in those areas.

Dollar Losses

According to a 1974 survey conducted by the New York Times, losses to hotels and motels from theft alone exceeded $500 million. Although there are no industry-wide data measuring losses from property or personal crime, a comprehensive survey would likely reveal losses to be substantially greater -- given the vulnerabilities to loss present in the industry. Several factors are responsible for the lack of the much-needed industry crime loss data.

Records at the individual level frequently aren't kept, except where required for insurance purposes or where the operator recognizes the value of loss records as a crime prevention tool.

Reflecting the importance of public relations, it is not unusual for an operator to exchange a complimentary room or dinner pass for a customer's personal property loss. Although the value of the item stolen places an upper limit on the extent to which informal exchanges occur, records are not kept for losses handled in this matter.

Property losses -- that is, theft of assets belonging to the business -- frequently are not recorded, apparently because of the difficulty in pinpointing when, where and how the loss occurred. Hotel managers are reluctant to classify a loss as crime-related if there were other possible causes.

Vulnerabilities

An unlimited potential for property loss exists within the average lodging facility. For example, a partial inventory of operating units within an average hotel includes liquor storage, trash, purchasing office, refrigerator, staff dining room, linen, housekeeping staff office, valet office, employee's entrance, kitchen, refrigerators, lobby, bellboy office, cashier, dining room, executive offices, meeting rooms, caterer's office, caterer's storage, chef's office, and guest rooms.

Most of these areas are stocked with consumer goods with high resale or personal use value. Target items include food, liquor, office machines, linen, personal items, silver, china and glass. Administrative areas, such as payroll and registration, are stocked with records or money that present opportunities for employee theft, burglary, and robbery.

As is typical of most industry, the lodging industry is most vulnerable to property loss from its own employees. Although the New York Times survey cited above revealed that one out of every three guests stole property belonging to the hotel or motel, it generally is accepted by industry security experts that the great bulk of property loss is attributable to employees. The situation compares to increasing awareness within the retailing sector that shoplifting losses are relatively minor when compared to employee theft. The extent of employee theft in the lodging industry, as always, is a function not so much of dishonesty, but rather of the degree of opportunity and temptations present in the working environment. Two primary reasons account for risks to employee theft: (1) employee exposure to assets and (2) turnover.

Employees have a high degree of access to the assets of a lodging facility. The assets are sprawled throughout a facility and cannot be supervised at every point of access.

Annual turnover rates in the lodging industry are high, frequently exceeding 70 percent. The costs of continual prescreening, security orientation and refresher seminars associated with high turnover rates prohibits an effective personnel policy. As a result of erratic controls, employees have more opportunity to steal, and less compunction about doing so.

Fraudulent use of credit cards, checks and travellers checks is another area of vulnerability. As travel sales increasingly depend on these forms of payment, the risks associated increase. This type of crime is sometimes connected with another source of loss to lodging facilities: the "deadbeats" whose purpose is to obtain lodging on credit with no intention of paying bills. Most states how have deadbeat statutes or hotel fraud acts that make such fraudulent activity criminal.

Personal crimes against guests, such as burglary, robbery, assault, extortion, blackmain, murder and rape, result in losses in the form of increased insurance premiums, loss of reputation -- decreased occupancy, claim payments and lawsuits.

Many state laws specifically limit the liability of a lodging facility for theft of customer's property, if certain conditions are met. Most require, for example, that a safe for guest's property be provided and that a "conspicuous" notice be posted that such a safe is available. Most of these statutes also provide that the operator is not liable if the guest has not informed management of the excessive value of the items put in safe boxes. In addition, some statutes require installation of specific types of night bolts and latches on guest rooms.

Not all states limit liability, and losses to victimized facilities in these states can be substantial. However, even in states with limited liability statutes, the court will frequently disregard the statutory limit -- to the disadvantage of the hotel/motel operator.

The lodging industry is vulnerable to crimes against customers because of the difficulty in controlling access. The problem of screening out undesirable persons, specifically prostitutes and female criminals acting as prostitutes, is particularly difficult. The lodging facility obviously cannot regulate the morals of its customers, and is thus unable to successfully eliminate this type of crime. With regard to access control, industry sources also cite the complicating factor of potential libel, slander and discrimination allegations by persons refused access to a facility. The chances that legal actions will be brought -- even by persons legitimately refused entrance -- are sufficiently great to persuade some lodging facility managers to de-emphasize access control in favor of less-sensitive crime controls.

Opportunities for burglary of guest's property are greatest in the guest room. Robbery can occur anywhere the customer is isolated -- elevators, halls, rooms, lobby. These crimes are unpredictable as to when, where and how they will occur but perpetrators always take advantage of isolation.

Prevention

In one recent, well-known case, a jury awarded $2.5 million in damages to a guest injured on hotel premises. Later settlement diminished the value of the judgment to $1.4 million. Because of judgments such as these, negligence suits arising from personal crimes against guests have far greater impact on current security trends within the industry than does control of property losses.

The reduction in losses stemming from personal crimes is a sensitive issue within the lodging industry because of the unsettled nature of the law. The courts have not yet clarified what the operator's "duty to protect the guest" involves, nor have they specifically defined what constitutes "reasonable care," the exercise of which would decrease liability. Few lodging facilities can meet the stringent standard being adopted by the courts. The problem facing the industry is the fear of the unknown: how much has to be done to avoid liability in multimillion dollar lawsuits.

It appears that a first step could be controlling access, since most guest victimization is perpetrated by outsiders. One major hotel in New York City restricts access to the main door; persons entering the hotel pass by several employees trained to recognize unusual behavior. Access also can be controlled by situating registration desks or employees in strategic positions to monitor entrances.

Closed circuit television, alarms, or security officers are additional methods of controlling access. Facilities in urban and other high crime areas find combinations of these physical security measures beneficial, especially if *all* entrances are monitored. Cost/benefit analysis should be conducted before this type of security is installed, because the financial aspect can be burdensome to the small entrepreneur.

Many independent and chain facilities control access to guest rooms through elevator service control. For example, if a facility has five floors of special function areas, the following elevator schedule anticipates crime vulnerabilities: there is no service to special function floors unless there are functions actually being held; there is no service from the lobby to guest floors after a certain time of evening, without special request to registration desk personnel; and there is rarely service to the roof.

Key control also is important to access control. Some hotel and motel chains have eliminated key problems by installing electronic systems that use magnetic cards or computer controlled combinations instead of keys, although a majority of facilities are economically unable to install such systems. Those facilities retaining the traditional system of keys can maximize key control by: avoiding the indiscriminate issuance of keys, registering requests for duplicates and masters, and ensuring that departing guests return room keys.

In addition to, and in place of, installation of more secure lock systems, some facilities also install peepholes in the doors to guest rooms as further protection to the occupant.

Beyond access control, most operators have to develop personal crime prevention programs around unpredictable circumstances. Employees can be integral elements in an effective program to reduce losses stemming from guest victimization.

If employees are fully utilized in this effort, possibly the most essential areas in a facility are the registration desk and lobby. Personnel in these areas can be trained to recognize unusual behavior, although experienced con persons will prove elusive. Access control is enhanced if entrances are monitored and entering persons evaluated. Employee training should include the proper method of handling suspicious persons, since employees can offend legitimate persons by undue harassment.

Personnel can be instrumental not only in reducing the indirect losses stemming from personal crime, but can also reduce credit losses. Although losses from credit card fraud can be reduced through the same methods employed by any establishment accepting them, check fraud is more difficult to control in the lodging industry since a majority of checks are non-local. Nevertheless, check cashing guidelines must be established and those in Section II, page 109, are adaptable.

Effective property loss controls center on employer/employee relations. While developing a staff capable of decreasing guest victimization by keeping the premises protected, management must avoid creating circumstances that tempt employees to steal the assets of the company. Employee controls should reduce opportunity for employee theft while increasing protection for guests. Such a program is a delicate balance, and requires a program founded on employee relations.

There are two basic approaches to employee theft. Management can either control dishonesty or cultivate honesty through an aggressive program of participatory management that emphasizes 2-way communication and identity with the organization. Because most persons will remain honest if given the chance, emphasis should be on the latter approach. Dishonesty controls -- such as package and purse inspections -- are an effective supplemental system of checks and balances.

To develop an honest and reliable staff, the primary obstacle which prevents effective employee control -- excessive turnover -- must be overcome. Programs to reduce turnover can be aggressive and innovative.

One major hotel in Los Angeles reduced turnover to under 50 percent through a program that emphasizes employee relations from application through hiring to termination. Special attention is given to orientation -- in both security and other organizational philosophies and regulations -- and training. Training is conducted in-house and outside and includes sessions on check and credit card acceptance procedures for registration desk employees. Employees are routinely evaluated and there is an in-house promotion program that gives employees an incentive to remain with the organization.

A Houston hotel experienced a turnover of 195 percent in 1971, the first year of operation; through a similar program based on participatory management, turnover was reduced to 80 percent by 1975. Fringe benefits include complimentary rooms at any other hotel in the chain after a year's employment. Additional incentives include employee of the year awards.

Another important element in reducing turnover rates is screening potential security risks during pre-empolyment phases. This is especially important in an industry where employee's exposure to assets is high. Industry sources cite the difficulty in reconciling the contrasting principles of privacy and civil rights legislation and pre-employment screening as a major problem in designing comprehensive security programs. The pre-employment screening suggestions and the summaries of Federal and State laws contained in Section II address this problem. In addition to standard procedures, outlined in Section II, precautions should be taken to avoid hiring floaters, employees who move from one hotel to the next as they are dismissed for disciplinary reasons.

Although dishonesty controls should supplement the more positive approach outlined above, they should not be discarded entirely. Typical dishonesty controls include irregular package and purse inspections as employees leave the premises, and a standardized approach to master key control. In unionized establishments, dishonesty controls usually are contained in contracts, and in any event, should be designed in cooperation with union representatives or employees.

Summary

The impact of crime on the lodging industry is severe enough for it to be an attributable cause of establishment failure, according to one industry source. Given the nature of the service produced, and the extraordinary vulnerability to crime, this industry should act more progressively in preventing the opportunities that create crime. The uniqueness of the service does not exempt its crime from the preventable category.

To control what surely will be escalating crime, the industry initially must develop a loss measurement and analysis approach. It also must overcome the fear that customer alienation will result from application of progressive security policies. In succumbing to this rationale, industry managers overlook both the public concern over crime and the industry capacity to ameliorate the impact of crime control through public education.

CHAPTER 6

PROPERTY AND CASUALTY INSURANCE SERVICES

There are approximately 2,890 insurance companies selling some form of property and liability insurance in the United States. Premiums written by these companies totalled $59.5 billion in 1976, while the industry suffered its third largest underwriting loss -- $2.3 billion -- of its history.

The function of property and liability insurers is basically to compensate victims for losses caused by the insured. Routine elements of claims encompass property damage, medical expenses, lost wages and special out-of-pocket expenses.

In an analysis of crime in the sector, it appears that insurance is second only to financial services as a source of ready cash for those in need. Fraud is not a new phenomenon to insurers, and criminal fraud is a major concern of the vast majority of insurers.

The insurance industry is atypical of the sectors examined in this report in several significant areas. Primary risks to crime losses are readily identifiable, unlike other service industries where major losses result from an infinite variety of schemes. Because of the identification of major risk areas, prevention capability is greater than in most other industries.

A second contrast is that employee dishonesty is not considered to be a primary factor in crime losses. Industry executives discount embezzlement or other internal fraud as a serious potential source of crime loss. The majority of loss is perpetrated by outsiders, by professional claim swindlers, organized crime or amateur swindlers in need of money. A significant percentage of outsiders are doctors, lawyers and other professionals. Internally, the employee with the greatest opportunity is the claims adjustor. So skillful, however, are professional swindlers that rarely is the claims adjustor an integral element to the insurance fraud perpetrated by the full-time swindler.

Significantly, despite the almost complete computerization of the industry, insurance executives discount the risk of computer abuse. What would appear to be a rather potent source of loss -- theft of data -- is not considered as such. One reason enabling the major insurers to discount the risk of computer abuse is the comprehensive controls over computer operations. At least one major insurer indicated that its computer operation was protected by those controls outlined in Section II, page 117,. Industry executives also consider the threat of computer destruction through actual sabotage sufficiently severe to warrant concern over physical safeguards such as placement of the unit.

Lastly, the industry is cohesive and benefits from an organization, Insurance Crime Prevention Institute, established solely to counter the most prevalent and costly crime that impacts upon the industry -- claims fraud. Although each individual company is hesitant to reveal techniques of claims fraud detection, for obvious reasons, it is apparent that a significant degree of internal cooperation exists that includes training and public relations programs that result in an affirmative exchange of ideas in loss prevention.

Insurance services treat criminal fraud in a progressive manner. As in other industries, criminal prosecution was the exception until the last decade. Insurance companies, having discovered a fraud, contented themselves with restitution. This, of course, freed the criminal for subsequent fraud. Companies now opt for apprehension and prosecution. Insurance services are aided by a plethora of state and Federal criminal statutes that impact on insurance fraud and facilitate prosecution. Fourteen states now have statutes making insurance fraud a felony.

Losses

The U.S. Chamber of Commerce estimates that the industry loses in excess of $1.5 billion annually to fraudulent claims. Most of the industry accepts this figure. One out of every ten claims filed is fraudulent to some degree; the cost of premiums to the public is inflated by at least 15 percent to compensate for the widespread victimization.

There is no adequate breakdown of the loss figure into greater detail.

Claims Fraud Vulnerabilities

Insurance companies face potential fraud on any type of claim. Major risks exist on auto damage, personal injuries and fire claims. The most common schemes used to perpetrate these frauds, according to the Insurance Crime Prevention Institute (ICPI), are staged and phantom accidents, body shop frauds, ambulance chasing, and arson.

A swindler stages an accident most commonly by using predamaged, stolen or rented cars to crash into another car operated by other swindlers. Both property and personal injury claims are contrived through staged accidents. Fictitious or inflated claims stemming from a real accident usually are filed by the numerous passengers that are in the second vehicle. It is not unusual to have as many as 10 to 11 personal injury claims from one staged accident, since from the swindlers' point, more passengers translate into more money. Rental cars are used frequently to stage accidents and occupants submit injury claims to the rental company's insurance carrier. These staged accidents require subsequent medical and mechanical collusion to substantiate the injuries.

Phantom accidents give rise to claims based purely on fictional happenings and can be contrived in numerous manners. For example, the swindlers can file a police report of a minor accident on private property that does not initiate physical investigation by the police because of its minor nature. Most successful phantom accidents depend on either the cooperation of doctors and body shop mechanics to produce the necessary documentation or the swindlers' ability to buy the documentation, or forge it on stolen letterheads and forms.

Body shop frauds are particularly insidious because a dishonest, skilled mechanic can transform non or slightly damaged vehicles into seemingly destroyed ones. "Cosmetic surgery" is done either with a sledgehammer or with damaged parts. Some body shop owners actually keep files of spare damaged parts for substitution with undamaged parts on an accident vehicle.

Although the ambulance chasing lawyer faces disbarment and criminal prosecution if caught, apparently the sanctions have not been effective deterrents, as the ambulance chasing scheme continues to flourish. A study conducted during the 1950's indicated that 85 percent of all accident victims were contacted by an unethical attorney. This percentage probably has remained constant in the twenty years elapsed since that survey was taken.

Although the practice remains pervasive, its format has evolved. Ambulance chasers now employ "runners" or "cappers" who do the actual ambulance chasing. Ambulance chasing can also be done by policemen, physicians, garage mechanics and other interested bystanders. The motive generating the scheme is the kickback or payment the chaser receives from the attorney. Runners cruise in cars equipped with powerful radio scanners, constantly monitoring police calls for reports of

CONTINUED

1 OF 2

traffic accidents. The use of such radios greatly expands the territory open to the runner.

The scheme is played out by approaching a slightly injured victim, usually disoriented and confused due to the shock of the accident, and offering legal aid. Once the victim accepts by visiting the attorney, a retainer is signed and a referral to a physician or mechanic is the next step. The damage -- whether personal or property -- is invented or inflated. Documentation for the fraud also can be purchased or forged. The inflated damages paid by the insurer are split between the scheme perpetrators. Rarely does the victim receive more than that originally entitled to.

The line between a fraudulent and an unethically inflated claim is often difficult to discern. Many lawyers have clients who find it hard to obtain a settlement on a minor claim for property damage alone. Lawyers, sensitive to the desire of insurance companies to avoid litigation on a personal injury claim, can exploit this weakness by exaggerating a client's injury -- of which the client was perhaps unaware -- merely to ensure compensation.

Arson for profit has a serious impact on the insurance industry. As one of the least detectable, least prosecuted crimes, arson is extraordinarily difficult to combat. The crime itself destroys the evidence and witnesses -- if there were any. Usually, there aren't. Arrest rates do not exceed 1 percent; prosecution of the 1 percent does not exceed 1 percent.

The abysmal arson detection statistics are magnified by the scope of the problem. The Insurance Services Office estimates that total actual arson loss in 1976 could exceed $4 billion. The National Fire Prevention and Control Administration, U.S. Department of Commerce, estimates that the impact of arson is as much as $10 billion if higher insurance premiums, lost jobs, higher taxes and higher prices for what is not burned, are included. This cost, however, excludes the loss in human lives that reaches as much as 1,000 annually.

Other, perhaps more reliable, estimates place the arson loss at $1.4 billion. This figure is more consistent with fire statistics compiled by the industry.

Incendiary fires account for 20-25 percent of all fires, and 40-50 percent of dollar losses. These losses exclude fires of undetermined origin. Fire investigators assert that 60 percent of unknown origin fires, which actually outnumber arsons and are ranked in fourth place by the Insurance Information Institute on a list of categories of fire causes, are actually arson.

Arson losses have increased in the past years due in part to the economic recession. Business persons with difficult financial problems often view arson as a way out of those financial difficulties. As an indication of the stimulus given to arson by the poor economy, arson rates increased over 70 percent per year for the last two years. Normal increases are approximately 10-15 percent.

Arson for profit covers property the claimant either did or did not own. Often, the arsonist/claimant removes the property -- office equipment, for example -- prior to burning the building. Frequently, the business person resorting to arson claims losses for fictional inventories.

Although auto accidents, ambulance chasing and arson are the most prevalent frauds -- and the most costly -- many other frauds do exist. Despite the apparent unconcern by major insurers, the dishonest claims adjustor has much latitude within which to inflate or invent claims, especially if the auditing controls are lax. Insurers who do not employ their own adjustors, using instead free lance or other services, would appear to run more of a risk.

Other common frauds, such as slip and fall accidents, burglary frauds, and domestic arson are perpetrated by individuals well versed in the techniques of insurance fraud, according to the ICPI, and are more conducive to detection.

As can be seen from a discussion of common schemes, there are key persons essential to the successful fraudulent claim. Doctors, lawyers, and garage owners are primarily movers. Many rings exist that combine all three in a complex, large scale fraud ring which is very difficult to track and stop.

Another element frequently present in lucrative, well conceived insurance fraud rings is organized crime. The ICPI indicates organized crime is prevalent -- from established syndicates to small, independent rings -- especially in staged and phantom accident schemes.

But, according to ICPI, the most successful rings are those led by doctors and lawyers who convert a legitimate, minor claim into a settlement that is five or six times above the original worth.

Fraud Prevention

Claims fraud is a very difficult crime to detect, much less prevent. More so than in other industries, the prevention flows from continually improving detection. When drafted by a skilled swindler, a fraudulent claim can easily pass examination by a veteran claims adjustor. The undetectability of claims fraud is perhaps the greatest threat to the insurance industry.

Through improved detection capability -- the essence of crime prevention -- insurance firms are able to develop internal policies that minimize the potential for payment of fraudulent claims. Significantly, however, individual insurers are able to reinforce internal policies with an industry-wide program that has been developed to focus on investigation, apprehension and prosecution of suspected swindlers.

Internally, the most valuable deterrent of an insurance company is a skilled and experienced claims adjustor, trained to be sensitive to swindlers' techniques. Such sensitivity alerts the claims adjustor to unusual (or too usual) elements of claims.

Prominent examples of items easily caught by experienced claims adjustors are distinguishable patterns, such as an individual with a history of claims involving the same injury. The behavior of the claimant can also provide clues to a potential fraud. Claimants who harass insurance adjustors for quicker payment, or claimants unusually well versed in insurance matters perhaps have ulterior motives.

Because claims adjustors are the company's first-line defense against payment of fraudulent claims, it is imperative that they be thoroughly trained in all aspects of potentially fraudulent claims. Many major companies, in recognition of this need, emphasize the claims fraud problem through in-house training programs.

An additional source of information to the claims adjustor is the Index Bureau System, maintained by the American Insurance Association. Subscriber companies submit such pertinent information as names of claimants, doctors, attorneys, type of injury and specifics about the accident on all claims filed with the company. The System allows claims adjustors to obtain a history of the other claims of the subject currently being investigated, as the indexing involves substantial cross indexing.

Use of the Index can reveal, for example, schemes of professional claimants -- those with an inordinate number of previous accidents. Another use of the Index can be to expose unethical attorneys, or attorneys working in collusion with physicians. An analysis of claims filed by particular attorneys can provide invaluable insight into fraudulent claims.

Internal auditing is imperative for the insurance company. Most major insurers provide control over claims adjustors, for example, by contacting claimants with audit letters. These purport to verify the actual amount of money received by the claimant in payment for an injury, and of course are useless if the claimant is a professional swindler. The returns on the letters frequently reveal fraud, after comparison with the company records. They can be invaluable and should be a routine element to the loss prevention policy of the company, subject to the limitation mentioned.

The second effective tool available to the insurance industry is the Insurance Crime Prevention Institute (ICPI). Addressing the problem of property and casualty insurance fraud through a vigorous program of criminal prosecution, public education, and industry training, the ICPI is an industry wide prevention organization.

Over 320 property and casualty insurance companies refer suspicious claims to the ICPI for investigation. Activities do not extend to life insurance fraud. In furtherance of the deterrence objective, it will not investigate any claims for which the insurance company is interested only in obtaining restitution. Since its inception in 1971, over 2,200 arrests have resulted, with a 90 percent conviction rate of those actually tried from over 2,500 referrals. Still to be overcome, however, are significant problems with light sentencing of convicted swindlers. Dealing with the insurance-related crimes of larceny, obtaining money by false pretenses, forgery, perjury, using the mails to defraud, and ambulance chasing, this industry-wide organization is illustrative of an innovative and timely anti-crime program. Few other, if any, industries participate in such a concerted effort to reduce the impact of crime.

Regardless of the nature of the fraud, each insurance company must cooperate with law enforcement and prosecute swindlers. This requires a knowledge of the crimes -- whether using the mails to defraud, forgery, theft, false application -- and knowledge of the evidence required for successful prosecution. It also requires knowledge that claims fraud is a significant source of loss to the industry and to the public.

The insurance industry is unique in that knowledge of the problem is far more advanced than in other industries. Despite the reluctance of major insurers to reveal insight into prevention techniques, it is apparent that prevention is highly developed. Judged by the efforts of the ICPI, prevention is anticipatory and directed at improving the first line of defense -- claims adjustors -- to avoid the loss, without resorting to after-the-fact apprehension, prosecution and restitution. Other industries would do well to examine the approach taken by insurers.

Sources:

1. Insurance Crime Prevention Institute
   15 Franklin Street
   Westport, Connecticut   06880

2. National Fire Prevention & Control Administration
   2400 M Street, N.W.
   Washington, D.C.

CHAPTER 7

MISCELLANEOUS SERVICES

Although only a limited number of services were examined in detail in this study, crime is by no means limited to these six, as few services are exempt from the varied and severe impact of crime. A discussion of crime's impact on miscellaneous services follows. The crime problem of these services may or may not exceed those services given expanded treatment in the preceeding chapters, but the sparse data hampers detailed analysis.

Construction Equipment Distributors

Construction equipment distributors, surveyed by Associated Equipment Distributors, estimated losses in 1970-75 to exceed $500,000 for stolen machinery. This amount, which is dwarfed by losses in other individual industries, is put in better perspective by the great difficulty in stealing a 15,000 ton tractor. Almost 50 percent of dealers surveyed responded affirmatively when asked if crime was a problem.

According to industry sources, stolen machinery is rarely recovered, and thieves are rarely caught, despite the size and identifiable characteristics of the machinery. Significantly, most of the thefts occur from the distributor's own yards, rather than the rental site as one might expect. The problem is perpetuated by the ease of absorption of machinery into the market and is further compounded by law enforcement's unfamiliarity with machinery and its identifying characteristics, as well as by the professional methods of stealing which indicate involvement of organized crime.

To rectify these major problems, the industry association has initiated development of a manual for law enforcement personnel that facilities identification of various types of machinery, through description and profile sketches. Industry executives also urge the development of a better internal reporting system and improved cooperation with law enforcement personnel.

Coin Laundry Equipment

Another service vitally concerned with crime losses is coin laundry operators, who, for example, provide the laundry equipment in multifamily living complexes. There are two primary vulnerabilities to losses. First, employee theft and robbery are risks during collection of money from the machines. Second, the professional lockpicker is a significant threat in the interim between collection.

A recent release by the National Association of Coin Laundry Equipment Operators estimated that the average professional lockpicker steals $120,000 annually from laundry machines, alone. Unfortunately NACLEO did not estimate the number of professional lockpickers, although it placed the loss at the multi-million dollar level.

Threats similar to those other industries cope with also exist. For example, pilferage of machine parts and tools occurs. Theft of entire machines is not uncommon, either from the installation site itself or from the owner's inventory.

The greatest risk, however, remains loss of money from machines. Collection risks parallel the risk retailers and other service entrepreneurs face in making routine daily bank deposits. That is, by establishing a pattern -- regular time, regular route, for example -- collectors in effect set themselves up for robbery. Such routines also establishes a safe time for professional lockpickers within which they can operate, with maximum take.

Moreover, unless cautious hiring of collectors is emphasized, and NACLEO recommends exhaustive pre-employment screening, loss risk in the collection phase of the business can be even greater.

The risk to loss perpetrated by professional lockpickers is inherent in the industry. There is virtually no pick-proof lock. Lockpickers, especially those operating professionally in a ring, with staked out territory, can be frustrated if equipment operators scramble the types of locks installed on their machines.

Airline Passenger Services

Another specific area with serious semi-defined crime problems is airline passenger services. Computer manipulation makes fraud relatively easy, especially if collusion exists between ticket agents and computer employees. Although no recent estimates are available, 1971 losses were estimated to exceed $10 million. Given the factors of (1) expansion of air travel, which results in increased volume of tickets and increased opportunity for fraud through mere volume, (2) the increasingly sophisticated computerization and (3) the annual increases in all types of crime impacting on businesses, it appears that the $10 million loss has at least doubled.

In addition to ticket fraud losses, airlines also experience significant risk to bad check losses. Earlier estimates indicate that approximately two-thirds of airline ticket business is done by check. Based on incomplete information, at that time bad check losses were estimated to be in excess of $7 million. Despite increasing use of bank credit cards, travel and airline charge cards, checks remain the predominant form of payment and thus bad check losses have increased in rough similarity to other losses.

Hijacking remains a viable threat to domestic air carriers, although infrequent. This crime is increasingly politically, rather than financially, motivated. There has been only one domestic hijacking attempt in the last three years. The anti-hijack measures imposed by Federal regulations have been responsible in large part for the abatement of hijack frequency.

Summary

There is little insight -- statistical or otherwise -- into crime losses into the remainder of the service trends. That crime exists is certain, for wherever money or goods exist, temptation to steal is near. A nonreported crime is nevertheless a profit drain and the lack of statistical paradigms for crime in many services does not alter the inescapable fact of its severe economic impact.

SECTION II

This section emphasizes specific crimes, preventive measures and issues with which business managers should become familiar. As policies are developed to reduce the economic impact of crime, it is important to understand the problems and be aware of alternatives. Management must anticipate crime, and be sensitive to the issues which often complicate prevention efforts.

In keeping with the primary objective of this report -- to increase management awareness of crime and to suggest strategies to reduce its impact -- this section is necessarily broad. Crime and prevention tools vary from city to county, state to state and business to business. These variations are recognized but detailed treatment is beyond the scope of this particular report.

Consult local law enforcement authorities for technical advice on crime prevention. For information about local prosecution requirements -- that is, evidence, witness, time schedules and similar procedural matters -- contact the district attorney's office. These local authorities should be able to advise; if fundamental questions are left unanswered, form local action groups to improve liaison and formulate working knowledge. Often, membership in local trade associations, local chambers of commerce, or boards of trade is beneficial to smaller businesses which lack sufficient resources to develop successful crime prevention programs.

The discussions that follow are intended to provide a broad framework for developing management policy that will reduce the impact of crimes against business.

EMPLOYEE THEFT

No matter what it is called -- internal theft; peculation; embezzlement; pilferage; inventory shrinkage; stealing; or defalcation -- thefts committed by employees are behind at least 60% of crime-related losses. So many employees are stealing so much that employee theft is the most critical crime problem facing business today.

Although employee theft results in part from factors beyond control, the extent of employee theft in any business is a reflection of its management -- the more mismanagement, the more theft.

Components of a "stop employee theft" policy must include, as a miminum:

--- pre-employment screening
--- analysis of where opportunities for theft exist
--- analysis of how employees steal
--- management-employee communication
--- prosecution of employees caught stealing

The task any employer faces is to reduce losses as much as possible. A police state needn't be created. Large monetary expenditures needn't be made.

PRE-EMPLOYMENT SCREENING

o The best way to stop employee theft is simply not hire those employees inclined to steal. The best way is also impossible. What the employer must do is to set up a screening process that will weed out obvious security risks. Many experts believe that personnel screening is the most vital safe-guard against internal theft.

o Some basic guidelines for the employer (because of the legal implications of the process, a separate discussion follows on employee rights and privacy):

--- Always have applicant fill out written application. Be sure that written application does not discriminate and is in conformance to any applicable laws. See samples on pages 105 and 106.

--- Exercise caution when considering ex-convicts for employment. (This is not meant to be a steadfast rule -- individual judgments must be made as to degree of rehabilitation.) It is illegal to solicit information about arrest records not leading to convictions.

--- Solicit references but keep in mind that those contacted will give favorable opinions. Ask primary references for secondary references. In contacting the latter, make it clear that the applicant did not refer you.

--- Always interview. In interviewing, assess the applicant's maturity and values. Observe gestures.

--- Use psychological deterrents -- inform applicant that your business routinely runs a security check on background, or that fingerprinting will be taken. The hope is that the dishonest applicant won't be back.

--- Obtain credit bureau report but only after following guidelines set forth in Fair Credit Reporting Act.

AREAS, METHODS AND CONTROLS

o Cases of employee theft have been documented in almost every conceivable phase of business operations -- from theft of petty cash to theft of railroad cars. There is an infinite variety of methods used.

<u>Areas Most Vulnerable</u>

--- shipping and receiving
--- inventory
--- accounting and record keeping
--- cash, check and credit transactions
--- accounts payable
--- payroll
--- facility storage units

<u>Methods Used</u>

--- pilferage -- one item at a time
--- cash register theft or alteration of cash register records
--- issuance of false refunds
--- use of back door, trash containers
--- taking advantage of under-supervision
--- avoidance of package control
--- embezzlement

--- check forgery
--- stealing credit cards
--- manipulating computers, stealing computer time
--- night cleaning crew
--- duplicating keys, or use of master key that is not properly controlled
--- collusion with outsiders, inflated claim in insurance, for example.

o Too many opportunities exist for employees to exploit -- reduce the opportunities and losses will be reduced. Reduce opportunities by control.

Useful Controls

--- randomly spot check all phases of business, in addition to regular, comprehensive audit
--- check payroll -- make sure you're not paying a fictitious or dead employee
--- take physical inventory seriously
--- know what you own -- be able to identify it
--- do not allow one employee to perform all functions. Separate receiving purchasing and accounts payable. Separate accountants from cash.
--- control payment authorizations
--- keep blank checks locked, don't pre-sign or use uncoded, unnumbered checks
--- reconcile cancelled checks with original invoice or voucher
--- secure exits -- restrict employees to one exit. Prevent exit from back. Establish strict package control.
--- inspect cash register receipts daily, inspect tape, ensure that employee is identified on slips, deposit monies daily
--- issue identification badges to decrease employee presence in unauthorized areas
--- simplify red tape -- make it harder for the employee to disguise theft
--- have employee parking away from business establishment
--- establish usage schedule of supplies to isolate irregularities.

MANAGEMENT - EMPLOYEE COMMUNICATION

o Leadership must be firm yet reasonable. Most employees pattern their values after yours, so a good example must be set. If you expect your employees to remain honest, don't cart home office supplies or goods.

--- Train new employees, advising them of the company's values and the standards by which they will be expected to perform. Explain all security procedures, stressing their importance. Emphasize that any deviations will be thoroughly investigated.

--- Establish a grievance procedure, and give your employees an outlet for disagreement and be receptive to all grievances submitted. Ensure that employees are aware of its existence and that no reprisals are taken.

--- Regularly evaluate employee performance and encourage them to evaluate management. Unrealistic performance standards can lead either to desperation and anger, resulting in dishonesty or to "get-even" attitudes. Regularly review salaries, wages and benefits -- dont's force employees to steal from you!

--- Delegate responsibility. Unless decision-making exists among lower and mid-levels, there is a tendency for an "it's us against them!" attitude to develop. Delegate accountability as well; no decision is valid if it is lost in a "buck passing routine."

PROSECUTION

Prosecution is sometimes expensive and slow, but if employee theft is to be reduced, dishonest employees must be prosecuted to the fullest extent of the law.

o Fear of apprehension and prosecution is often the best deterrent and when the threat of jail exists, there is a good chance the employee will think twice.

o Report all incidents to the authorities and cooperate with them.

o Establish liaison with law enforcement and District Attorneys -- know what evidence is required and what the procedures are.

o Find out if your community has a program for businesses that reduces the amount of time an employee witness must spend away from work to testify.

o Take an active role in urging tougher sentencing for embezzlers and other employee thieves -- who, after all, are responsible for more than 60 percent of the losses to crime.

EMPLOYMENT APPLICATION

AN EQUAL OPPORTUNITY EMPLOYER

NAME (Print) LAST FIRST MIDDLE

SOCIAL SECURITY NUMBER

ADDRESS (Street, Apt. No., City, State, Zip Code)

NO. YEARS

TELEPHONE NUMBER

PREVIOUS ADDRESS (Street, Apt. No., City, State, Zip Code)

NO. YEARS

Yes □ No □

CITIZEN OF USA?

Single □ Married □ Separated □ Divorced □

MARITAL STATUS

BIRTH DATE

SPOUSE'S NAME, EMPLOYER, & EMPLOYER'S ADDRESS

LIST ANY RELATIVES CURRENTLY OR FORMERLY EMPLOYED BY CORPORATION OR ITS SUBSIDIARIES.

LIST PHYSICAL DISABILITIES (if job related)

Name Address Telephone No.

IN CASE OF EMERGENCY, PLEASE NOTIFY

Position Desired

Salary Requirement

Date Available

Referred By Whom?

Previous Resume or Application on File?

Dates

Service Number

Branch

Rank at Separation

UNITED STATES MILITARY SERVICE

EDUCATION

Type of School	Name and Address of School	Courses Majored in	Circle Last Year Completed				Graduate? List Degrees	Units Completed	Years Attended	
									From	To
Elementary			5	6	7	8	□ Yes □ No			
High School			1	2	3	4	□ Yes □ No			
College			1	2	3	4				
College				2	3	4				
Graduate School			1	2	3	4				
Business or Trade School			1	2	3	4				
Correspondence or Night School			1	2	3	4				

Do you hold any professional registrations and/or licenses? Yes □ No □

Do you hold any patents? Yes □ No □

Have you ever had a book or paper published? Yes □ No □

Extracurricular Activities (Civic, Athletic, Fraternal). Do not include religious, racial, or national origin groups:

List your last employer first. Account for all occupied and unoccupied time for the past ten years. Show dates and addresses on for periods of unemployment.

A. EMPLOYER'S NAME B. ADDRESS & TEL. NO.	DATES EMPLOYED		POSITION	SALARY		REASON FOR LEAVING	IMMEDIATE SUPERIOR
	FROM	TO		START	FINAL		
	MO. YR.	MO. YR.					
1. A. B.							NAME: TITLE:
2. A. B.							NAME: TITLE:
3. A. B.							NAME: TITLE:
4. A. B.							NAME: TITLE:
5. A. B.							NAME: TITLE:
6. A. B.							NAME: TITLE:

Indicate by number any of the above employers whom you do not wish contacted ______

Why? ______

Indicate below your office skills and the office machines you can operate efficiently.

Typewriter: Electric — Shorthand: Speed ______ — Calculators: ______

Speed ______ Standard — Speed Writing: Speed ______ — Duplicators: ______

What languages do you speak, read, or write fluently? ______

REFERENCES

(Exclude Relatives or Former Employers)

NAME	ADDRESS & TELEPHONE NUMBER	BUSINESS	YRS. KNOWN
1.			
2.			
3.			

In the event of my employment by the Company, I agree to abide by all present and subsequently issued rules of the Corporation. I authorize all schools which I attended and all previous employers to furnish Corporation with my records and release Corporation from all liability for any damage whatsoever arising therefrom. I also authorize investigation of all statements in this application, which can include verification of birthdate, military service, and citizenship status, if employed. I further understand that Corporation may make inquiries into my background for the purpose of establishing my character, general reputation and personal characteristics. Also, I understand, in the event of employment by the Corporation, I shall be subject to dismissal if any of the information I have given in this application is false or I have failed to give any material information herein requested.

Date: ______ Signature: ______

Hired: ______ Dept.: ______ Position: ______ Reports: ______ Salary: ______

(Interviewed by: ______

EMPLOYEE RIGHTS AND PRIVACY

An integral element to protecting a company from internal crime is personnel security controls. The most basic control is pre-employment screening. In recent years, inequities in our society, combined with an emphasis on individual rights, has prompted legislation that is directly relevant to an employer's pre-employment screening process. To facilitate identification of the more important legislative actions, a summary of existing Federal and State laws follows.

Federal Laws

Many Federal laws impact on an employer's pre-employment screening process, although most apply only to employers with 15 or more employees. Employers should be familiar with their provisions and cognizant of the risks associated with their violation. This is particularly important because discrimination does not have to be intentional for an employer to be in violation of the law.

Title VII - The Civil Rights Act of 1964 bans discrimination. It is not illegal per se to ask race, color, creed, national origin or sex, but such inquiries will be viewed as evidence of discrimination if there is no logical explanation. This legislation extends to all phases of an employee/employer relationship through recruitment to termination, and is the basic source of anti-bias employment.

The Age Discrimination in Employment Act of 1967 bans discrimination on the basis of age. Inquiries about age (date of birth, graduation) have been considered evidence of discrimination against applicants in protected age groups -- 40-65 years of age.

Fair Credit Reporting Act regulates methods of obtaining applicant's credit bureau report. (1) applicant must be informed in writing that report is being sought; (2) applicant must be told what type of information is being sought; (3) if applicant is denied a job solely on basis of report additional disclosures must be made.

The Privacy Act of 1974, designed to deter collection and prevent dissemination of personal information by the Federal government, restricts business executive from obtaining criminal information about an applicant, forcing reliance on the public record. Don't hesitate to consult the record whenever possible. It <u>can</u> be informative.

Many other Federal laws exist -- regulating inquiries about everything from pregnancy to facial characteristics. The Equal Employment Opportunity Commission (EEOC) issues guidelines affecting screening as does the National Labor Relations Board, the Department of Labor, and other Federal agencies. It is advisable that an employer seek legal counsel to find out exactly what the position is with respect to Federal law, especially since this area is the subject of constantly evolving judicial and legislative interpretations.

State Laws

Every State has a civil rights act that impacts on prescreening procedures. Most ban pre-employment inquiries inferring discrimination on basis of race, color, religion, sex or national origin. Each State does have different legislation -- thus it is imperative for the employer to become familiar with the provisions of that law. Discrimination lawsuits can be expensive.

BAD CHECKS

Ninety percent of the volume of business in the United States is done by check. Over 29 billion checks are drawn on 100 million checking accounts at the 14,000 plus banks in operation.

The sheer magnitude, alone, of the volume of business conducted by check indicates that risks of losses due to the misuse of checks are abundant and present a serious problem to any businessman.

The estimated total cost of bad checks exceeds $1.3 billion. This includes the actual amount of checks -- an average bad check is $30 -- and the cost of collecting -- an average $10.

Small business suffers losses 3 times greater than the average of general business and 35 times greater than large business.

There, are, in essence, two approaches to the solution -- individually and collectively. We recommend that the two approaches be combined for maximum effectiveness.

The Basics of an Individual Approach

- The easiest solution to bad check losses is to stop accepting checks. But in view of the competitive nature of the marketplace and the importance of service, this solution is, of course, impossible.

- You must establish a policy that reduces your losses as much as is possible while maintaining your status. Basic rules that any policy should cover:

  - Do NOT cash, or accept for payment, checks without 2 proper ID's.
    MAKE NO EXCEPTIONS.
  - Do NOT cash checks for more than purchase.
  - Do NOT accept non-imprinted, or counter checks.
  - Do NOT accept post or past dated checks.
  - Do NOT accept certified or cashier's checks.
  - Do NOT accept two or more party checks, including payroll checks.

- Do NOT accept checks with alterations.
- Do NOT accept advance payment and subsequently refund cash without verifying check; if no verification is possible, ask customer to write new check for exact amount.
- Restrict check cashing to one specified area -- registration desk, business office, for example.
- Ask for second endorsement on check already signed when presented for payment.
- Do NOT accept non-local checks; in lodging facilities, Do NOT accept foreign checks.
- Do NOT take shortcuts around check cashing.

ID's

o These ID's are acceptable: current in-state driver's license; major credit cards (bank and otherwise); national retail credit cards; employee ID's with photos.

o Do not accept: social security cards, gas credit cards, library cards, membership cards, etc.

o Contributing to losses is the use of false identification. To minimize the problem, accept only above mentioned ID's. An in-state drivers license is familiar -- be wary of out-of-state drivers licenses. There is no uniform standard in the U.S. for licenses, so the variety in form and content of each makes it difficult to detect false out-of-state licenses.

o Always verify signatures, comparing signatures on both ID's with the check. If there is even the slightest doubt, reject the check.

Advertise Policy

o Post your policy in more than one location, alert all customers.

o Train employees. Discuss policy, stress no-exceptions, alert them to methods and techniques check passers use.

o Formulate a guide for employee's use. An example is on p. 113.

o Stress priority of your check policy to employees. Some businesses feel that a successful deterrent is to make employees who deviate from the policy responsible for resulting loss.

Collective Approach -- Community Policy

o If only a few businesses establish strict policies, results reflect in loss of competitive status and business. Most customers do not yet appreciate efforts to reduce losses, seeing them as a "hassle," and "an insult to integrity."

- Establish a community wide standard. If all merchants and services enforce similar policies, consumers can't complain of harassment.
- Set up a standard through your local Chamber of Commerce, Better Business Bureau or merchants association.
- Precede policy with an advertising campaign; alert the community, thereby reducing consumer resistance.

Additional Insurance

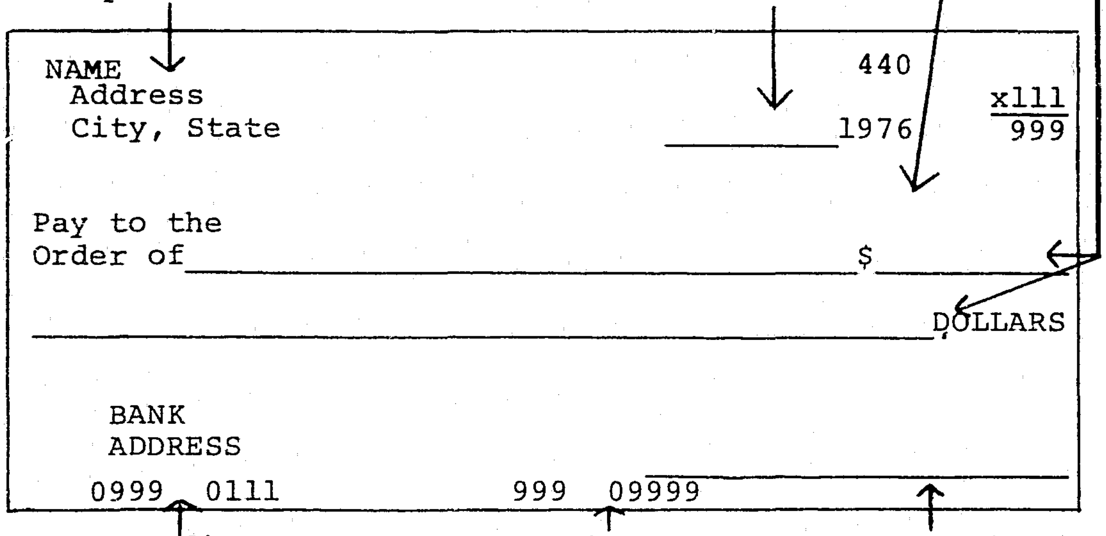
- Camera systems photograph the writer along with ID's and check. Develop film only when the check is returned, and send to writer for collection.
- Dry thumbprint methods enable thumbprinting of the check writer and aid in apprehension of bad check passers.
- Computer systems allow instant on-line verification. Other commercial systems are available that involve telephone connections to check data banks.
- "Fanout" system. Alert neighbors to bad check passer, form a chain. Help potential victims be on the alert.
- Cooperate with local, state and federal law enforcement authorities; report your bogus checks, and false ID's.
- Above all, realize that loss from credit card and check fraud can be reduced greatly -- _if_ an intelligent, logical approach is taken.

Local?
Imprinted?

Post or Past
dated?

Alterations?

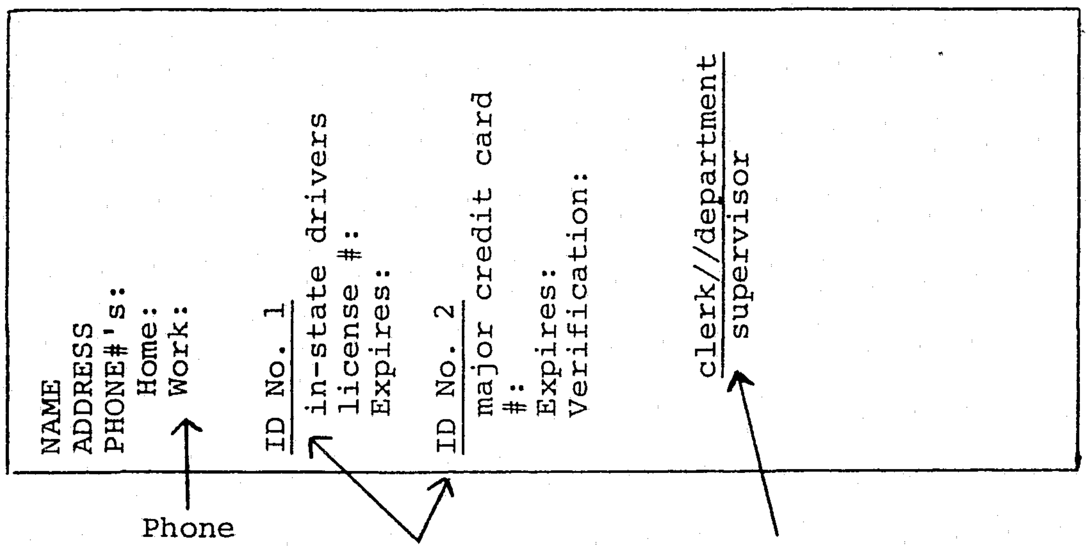
Agreement?



Encoding agree
with that by date
in upper right
hand corner?

Verify account
with bank

Check signed
in your pre-
sence?



Phone
numbers?

2 ID's?
Current?
Signature check?

Who handled
sale? Additional
verification?

CREDIT CARD LOSSES

Sixty-five million credit card transactions are recorded annually. In 1974, BankAmericard and MasterCharge, alone, had gross billings of $17.6 billion. Consumers pay for goods and services with over 500 hundred million credit cards.

The trend in business transactions is toward the use of credit, as technology develops increasingly sophisticated devices that make cash obsolete. Credit payment exposes merchants and service providers to a high degree of vulnerability because of the many possibilities for fraudulent use.

But, as is the situation with payment by check, an establishment that accepts payment by credit card risks high losses only if proper procedures are not followed.

Most major credit card companies offer a verification service to their clients. Use it. It is this service that affords greatest protection. Before accepting any credit cards, the "hot sheet" or "hot line" must be checked.

Other essential controls include:

- do not accept without proof of identity
- do not accept without signature verification
- do not accept expired cards
- make sure card imprint appears on all copies of invoice
- train employees on proper handling of credit cards and take advantage of free clinics sponsored by major credit card companies
- prosecute customers or employees responsible for credit card fraud
- alert authorities immediately to bogus cards -- and alert fellow business executives.

These controls do not afford protection against employee misappropriation of credit cards. The most popular methods used are a record of charge for a cash sale after credit has been established, or "forgetting" to return a card after customer has paid. Employee abuse leading to credit card loss can be reduced through application of measures that reduce opportunity for employee theft -- strict employee controls and training.

COMPUTER CRIME

Crime by computer contributes more and more to the annual costs of crimes against business. Because the technology is itself sophisticated, management faces a difficult problem in trying to prevent the crime. Moreover, a computer crime is subtle, invisible, and not subject to conventional auditing. Management must exert additional efforts to both understand the computer and prevent criminal abuse of it.

The computer remains a novelty for many business executives. But its crime is deadly serious and the criminal is highly skilled. The computer operation of a facility is the area with the greatest crime potential, in dollar terms.

There are fundamental elements necessary to an understanding of a computer:

- A computer does not operate independently. Operated by people, it depends on those people. So the computer is not infallible and a force unto itself.

- A computer stores and utilizes data. A criminal does not need cash or goods to defraud -- trade secrets, sales data and personal data can be intercepted. Moreover, by manipulating data, whole inventories can be stolen very easily.

- Because computers do exactly what they're told, a system can be sabotaged to destroy the whole company by delayed action. An altered program instructing the system to self-destruct at some future time (weeks, months, years) is possible.

- A criminal need never be physically present to abuse your computer system.

- A computer jargon is just that -- jargon. To understand a computer, it's not necessary to converse in the jargon.

There are more than 110,000 computers in use today, excluding remote terminals. Although few cases of computer crime are documented, it is estimated that for every detected computer crime there are 100 undetected crimes in progress. Furthermore, another estimate indicates that for every five computer related crime detected, four go unreported. The annual data loss attributed to computer-assisted crime is therefore difficult to ascertain with accuracy. It has been estimated, however, that the loss resulting from average computer-assisted embezzlement is ten times higher than the average $100,000 loss from traditional embezzlement. Dollar loss for one incident has been as high as $5 million, as reported by the U.S. Chamber of Commerce.

Vulnerabilities

According to some industry experts, a major share of computer abuse results from carelessness. Employee dishonesty is the second major cause. Remote terminal manipulation is currently a lesser cause, but has the greatest potential.

Losses can be in the form of (1) denial of essential service (2) compromise (3) misuse and (4) theft of material (tapes, etc.). The crime itself can be almost any traditional crime, such as embezzlement, inventory theft, or fraud, as well as complex schemes involving misappropriation of computer time, theft of programs, and illegal acquisition of proprietary information, such as trade secrets and industrial espionage.

Force attacks (sabotage) have declined from their peak in 1969-1970, due to both increased emphasis on physical security and decreased tensions within the elements of society responsible for computer attack during the 1960's.

On the other hand, embezzlement by computer is increasing and forms the majority of criminal incidents. Due in part to the technology itself, this type of computer abuse has proved relatively easy for a number of reasons, including: (1) top management tends to disassociate itself from computer systems due to lack of understanding; (2) all records are centralized; (3) there is no paper trail -- no trace that a crime has been committed; (4) there is a generally lax attitude concerning all phases of computer security; and (5) not enough caution is exercised in hiring and training personnel in managing computer work.

Specifically, computer abuse can occur in any computerized phase of your operation.

o Payroll -- through creation of fictitious personnel and other means, payroll can be a great source of extra income.

- Accounts receivable -- loss of the computer records of monies owed can be devastating to a company, large or small.

- Inventory -- in an unsecure system, it's incredibly easy to create fictitious accounts and then falsify records to show bills were paid, all the while delivering the inventory to a fictitious warehouse.

- Disbursements -- through manipulation of data, a company can easily be tricked into the reverse of fraudulent delivery -- paying for goods and services never received.

- Operations information -- this data can be very valuable, containing personnel information, and growth plans, for example.

Analyze your organization for specific vulnerabilities, and understand the special sensitivities these areas represent to the assets of the firm.

Prevention

Management must evaluate the threats to its computer operations after vulnerability analysis and before constructing a security program. As in any security, it is unrealistic to spend more on protecting the asset than the asset is actually worth. To assess risks, consider the following factors:

--- property location and environment of the firm itself.

--- Employee and non-employee access to the computer facility -- including service and maintenance personnel.

--- Confidentiality of data stored in computer.

--- Exposure to natural disasters.

Following are very basic suggestions as to what should form a basis to a comprehensive policy implemented by the lay person manager. They do not deal with technicalities (as these matters are better discussed with computer security experts) and should not be substituted for expertise.

Learn about your computer

- Learn the language (or insist that discussions be in English).

- Learn to read print-outs and read them.

- Compare actual program with original program periodically -- not in fixed schedule.

- Develop systems measurement to record use of the computer, to reveal who uses it, when, for how long and for what purpose.

- Remember that computers accept all input as truth. Any computer can be made to prove that 2+2=5.

Make security a priority

- Advertise security precautions -- hardware, software and personnel.

- Control access to the facility -- whether remote or primary equipment. Issue and require display of photo ID that is visually coded for immediate personnel recognition. Apply regulations to vendors, maintenance and repair persons as well.

- Control access to data in storage -- be sure that computer system has ability to level the degree of access among users.

- Do not advertise the computer system -- and discourage idle talk about computer among computer and non-computer employees.

- Run spot checks on computerized payroll. Investigate ANY deviations.

- Control computer waste material and separate from "regular" trash. An outsider gains knowledge through pilfering trash.

- Install locks, alarms, etc. to deter forceful entry to physical facility. Do NOT, however, rely on these devices to prevent criminal abuse of your computer.

Know how to hire, train and dismiss employees

- Screen applicants carefully and train new employees, stressing security priority.

- Do not insulate computer operational staff from routine company policy.

- Insist that mandatory, annual 2-week consecutive vacations be taken by computer employees.
- Immediately remove departing employee from access to computer, regardless of the circumstances prompting departure.
- A computer is only as honest as the people who operate it. Remember that, and treat your personnel accordingly.
- Functions of programming, operating and controlling must be separated. No programmer should have access to the computer. His function is design -- not operation. Control must be independent of operators.
- No one person should EVER be in a position to have available all have all the pieces that can be put together to make a whole.

Special problems of remote terminals

There is little management can do to prevent their remote system being manipulated by someone 2,000 miles away -- an unfortunate predicament created by the widespread use of time-sharing, networking, multi-access systems.

- Consider use of scrambling but remember that computers decode as easily as they encode.
- Change ID password frequently and irregularly.
- Because passwords are extremely easy to obtain, consider hand geometry, voice pattern etc. as ID. Also consider the inconvenience associated.
- Don't use a multi-access system for storage of sensitive data.
- Maintain duplicates of transmissions.
- Above all, know what's going on in your own company by auditing frequently.

Summary

Not many years ago, computer crime was the crime of the future. The future has now arrived, and management of computerized businesses are faced with extraordinary challenges in preventing abuse of their computers. Management, however, must not consider the computer as a business tool exempt, because of its novelty, from controls that effectively reduce risks to other forms of employee theft and fraud. These controls are fundamental to the reduction and prevention of crime and computers can not be an exception.

Further Sources

Statistical

1. Uniform Crime Reports, Crime in the United States. Federal Bureau of Investigation.

   Printed annually, the 1975 issue is available from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402. #027-001-00013-1. $3.60.

2. Criminal Victimization Surveys, National Crime Survey Program, U.S. Department of Justice, Law Enforcement Assistance Administration.

   These surveys measure crime loss due to burglary and robbery in certain selected cities, including Atlanta, Baltimore, Chicago, Cleveland, Dallas, Denver, Detroit, Los Angeles, Newark, New York, Philadelphia, Portland and St. Louis.

   For availability -- there are different publications for groups of cities -- contact Law Enforcement Assistance Administration, National Criminal Justice Reference Service, Washington, D.C. 20531.

3(a) Air Freight Loss and Damage Claims,
(b) Quarterly Freight Loss and Damage Claims Reported by Common and Contract Motor Carriers of Property,
(c) Quarterly Freight Loss and Damage Claims, Class I Line-Haul Railroads.

   Available from Department of Transportation, 800 Independence Avenue, S.W., Washington, D.C. 20591.

4. Sourcebook of Criminal Justice Statistics - 1975. U.S. Department of Justice, Law Enforcement Assistance Administration, National Criminal Justice Information and Statistics Service.

   (Prepared through a grant project to 40 Criminal Justice Research Centers, this is a compilation of criminal justice and related statistics that are available from the publications of a variety of governmental and private agencies).

   Available from Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

   Specify Stock Number 027-000-00332-0. Price is $9.70.

General

5. Department of Commerce, Cost of Crimes Against Business, January 1976. This is currently being revised. The current issue is available from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402. Price is $1.60.

6. Department of Commerce, Crime in Retailing, August 1975. Available from Government Printing Office, Washington, D.C. 20402. Price is $1.10.

7. Department of Justice, The Criminal Use of False Identification, The Report of the Federal Advisory Committee on False Identification, November 1976. Available from Government Printing Office, Washington, D.C. 20402. Specify Stock Number 052-003-00226-4. Price is $6.30.

Non-Governmental Sources*

8. Security World Magazine
Subscription to this monthly magazine is available from Security World Publishing Co., Inc., 2639 So. La. Cienega Blvd., Los Angeles, California 90034.

9. U.S. Chamber of Commerce, White Collar Crime, 1974. Available from Chamber, 1615 H St., N.W., Washington, D.C. Price is approximately $2.50.

10. National District Attorneys Association, Economic Crime Digest. (Continuing series of publications.) Contact Economic Crime Project, 1900 L Street, N.W., Suite 607, Washington, D.C. 20036.

* Inclusion of these non-governmental sources should not be construed as approval, nor should the exclusion of others be construed as disapproval.

☆U.S. GOVERNMENT PRINTING OFFICE: 1977-240-848/341