NUREG/CR-1234
UCRL-52744

The Insider Threat to Secure Facilities: Data Analysis

J. M. Heineke and Associates

Lawrence Livermore Laboratory

Prepared for
U.S. Nuclear Regulatory
Commission

8007220024

NOTICE

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights.

Available from

GPO Sales Program
Division of Technical Information and Document Control
U. S. Nuclear Regulatory Commission
Washington, D. C. 20555

Printed copy price: $3.75

and

National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-1234
UCRL-52744
RS

The Insider Threat to Secure Facilities: Data Analysis

Manuscript Completed: May 1980
Date Published: June 1980

Prepared by
J. M. Heineke and Associates
Los Gatos, California

Lawrence Livermore Laboratory
7000 East Avenue
Livermore, CA 94550

Prepared for
SAFER
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555
NRC FIN No. A-0132

FOREWORD

This report was prepared by J. M. Heineke and Associates of Los Gatos, California under purchase order number 4910809 for Lawrence Livermore Laboratory (LLL).

We are indebted to: Jesse Snyder, chief of the intelligence section at the Federal Deposit Insurance Corporation (FDIC), and his staff for the bank fraud and embezzlement (BF&E) data; Donn Parker of Stanford Research Institute (SRI) International for the use of his computer-related crime files; personnel of the federal Drug Enforcement Agency (DEA) for the insider drug theft data; Richard Schechter of Lawrence Livermore Laboratory, who served as technical contact and assisted in collecting the bank fraud and embezzlement data; Cheryl Rose for her computational assistance; and Sallie A. Mullen of the Nuclear Regulatory Commission (NRC) for her valuable technical guidance.

CONTENTS

Foreword iii

List of Tables vii

Abbreviations and Definitions xi

Abstract 1

Introduction 1

Data Set 1: Bank Fraud and Embezzlement 3

Data Set 2: Computer-Related Crime 27

Data Set 3: Employee Drug Theft from Drug Manufacturers and Distributors 53

Appendix: DEA Regions 64

LIST OF TABLES

1. ABA deposit group numbers 5
2. Predicted losses, perpetrator position, and bank size . . . 7
3. Predicted losses, the number of perpetrators, and bank size 8
4. Predicted losses, employee bond coverage, and bank size . . . 9
5. Joint distribution of perpetrator position and method of detection: BF&E cases, 1976-77 17
6. Distribution of method of detection, conditional on perpetrator position: BF&E cases, 1976-77 17
7. Distribution of bank fraud and embezzlement cases by perpetrator position: 1976-77 18
8. Distribution of collusive attacks on banks, conditional on perpetrator position: BF&E cases, 1976-77 18
9. Distribution of conspiracy size, conditional on perpetrator position: BF&E cases, 1976-77 19
10. Distribution of number of perpetrators, conditional on bank size: BF&E cases, 1976-77 19
11. Distribution of method of detection, conditional on number of perpetrators: BF&E cases, 1976-77 20
12. Distribution of loss, conditional on bank size: BF&E cases, 1976-77 20
13. Distribution of perpetrator position, conditional on loss size: BF&E cases, 1976-77 21
14. Distribution of loss size, conditional on perpetrator position: BF&E cases, 1976-77 22
15. Distribution of perpetrator position, conditional on time concealed: BF&E cases, 1976-77 23
16. Distribution of time concealed, conditional on perpetrator position: BF&E cases, 1976-77 24
17. Frequency of detection by method 25
18. Distribution of perpetrators by type of group: BF&E cases, 1976-77 25

19. Distribution of group size: BF&E cases, 1976-77 25

20. Summary of Hobbs Act violations and extortion threats against banks as reported to FDIC: 1975-78 26

21. Predicted losses and the number and type of perpetrator 30

22. Predicted losses, victim institution, and type of perpetrator 31

23. Predicted losses, outside involvement, number and type of perpetrator 33

24. Estimated probabilities of success: reported cases 34

25. Distribution of position (by highest ranking perpetrator): computer crimes, 1958-77 37

26. Distribution of number of perpetrators: computer crimes, 1958-77 37

27. Distribution of type of crime: computer crimes, 1958-77 38

28. Distribution of victim institution: computer crimes, 1958-77 38

29. Distribution of crime category, conditional on perpetrator position: computer crimes, 1958-78 39

30. Distribution of perpetrator position, conditional on crime category: computer crimes, 1958-78 40

31. Distribution of loss size, conditional on perpetrator location: computer crimes, 1958-78 41

32. Distribution of perpetrator(s) location, conditional on loss size: computer crimes, 1958-78 41

33. Distribution of number of perpetrators, conditional on loss size: computer crimes, 1958-78 42

34. Distribution of loss size, conditional on number of perpetrators: computer crimes, 1958-78 42

35. Distribution of perpetrator position, conditional on loss size: computer crimes, 1958-78 43

36. Distributuion of loss size, conditional on perpetrator position: computer crimes, 1958-78 44

37. Joint distribution of number of perpetrators and perpetrator positions: computer crimes, 1958-78 45

38. Distribution of perpetrator position, conditional on number of perpetrators: computer crimes, 1958-78 46

39. Distribution of number of perpetrators, conditional on perpetrator position: computer crimes, 1958-78 47

40. Distribution of crime category, conditional on number of perpetrators: computer crimes, 1958-78 47

41. Distribution of number of perpetrators, conditional on crime category: computer crimes, 1958-78 48

42. Distribution of perpetrator location, conditional on crime category: computer crimes, 1958-78 48

43. Distribution of crime category, conditional on perpetrator location: computer crimes, 1958-78 49

44. Distribution of perpetrator location, conditional on victim institution: computer crimes, 1958-78 49

45. Distribution of crime category, conditional on victim institution: computer crimes, 1958-78 50

46. Distribution of victim institution, conditional on crime category: computer crimes, 1958-78 51

47. Distribution of case disposition, conditional on perpetrator position: computer crimes, 1958-78 52

48. Distribution of suspect dispositions: computer crimes, 1958-77 52

49. Relative importance of drug losses from manufacturers and distributors by type of incident, 1973-77 63

ABBREVIATIONS AND DEFINITIONS

BANK FRAUD AND EMBEZZLEMENT TABLES

Perpetrator Position

Executive: President, Chairman of the Board, Director

Top Management: Cashier, Senior Vice President, Operation Officer Trust Office, Treasurer

Low-Middle Management: Assistant Cashier, Vice President, Branch Manager, Head Teller, etc.

Staff: Teller, Clerk, Bookkeeping department employees, etc.

Method of Detection

Bank examination: Represents a state or federal examination.

Audit: Usually represents an internal audit, but occasionally indicates audit by outside firm.

Insider information: Indicates perpetrator was detected via information furnished by fellow employee.

Outsider information: Indicates perpetrator was detected via information supplied by individuals not employed by bank--usually a customer and often a customer complaint concerning his dealings with the bank or perpetrator.

Confession: Indicates both out and out confessions and errors on the part of perpetrator which led to confession.

Absence: Indicates perpetrator was detected while absent--usually on vacation or after death.

COMPUTER CRIME TABLES

Perpetrator Position

Executive

Cemp: Computer employee

Ncemp: Noncomputer employee

Unemp: Employee, position unknown

ABBREVIATIONS AND DEFINITIONS (Continued)

Corp:	Corporation
Outsider:	Nonemployee
Student	
Exemp:	Ex-employee
Unknown:	Unknown perpetrator

Crime Category

Phydest:	Physical destruction; facility, service, or hardware damage
Tinfo:	Theft of information
Tinv:	Theft of inventory
Datadest:	Data destruction
Thw/sw:	Theft of hardware and/or software
Nuse:	Unauthorized use of data and/or service
Fraud:	Fraud and/or embezzlement
Error:	Keypunch or computer error

Victim Institution

Fin:	Finance; banking, insurance, securities
Govt:	Federal, foreign, state, local government
Med:	Medical
Educ:	Educational
Salmfc:	Sales and manufacturing; chemical and pharmaceutical, petroleum
Compub:	Communications and publications
Tranutil:	Transportation and utilities
Compserv:	Computer service bureau, consulting, credit bureau
Proforg:	Professional organizations, labor unions, fraternal and political organizations
Ind:	Individuals

ABSTRACT

Three data sets drawn from industries that have experienced internal security breaches are analyzed. The industries and the insider security breaches are considered analogous in one or more respects to insider threats potentially confronting managers in the nuclear industry. The three data sets are: bank fraud and embezzlement (BF&E), computer-related crime, and drug theft from drug manufacturers and distributors. A careful analysis by both descriptive and formal statistical techniques permits certain general conclusions on the internal threat to secure industries to be drawn. These conclusions are discussed and related to the potential insider threat in the nuclear industry.

INTRODUCTION

This report provides both descriptive statistical measures and formal statistical analyses of three data sets. The data were gathered from industries that have experienced insider breaches of system or facility security. These breaches are, in one or more dimensions, analogous to threats potentially confronting managers in the nuclear industry. The industries from which the data were drawn are banking, drug manufacturing and distributing, and industries directly dependent upon electronic computing for accounting and inventory control.*

The first data set contains 313 cases of bank fraud and embezzlement (BF&E) with losses or potential losses of $10,000 or more reported to the Federal Deposit Insurance Corporation (FDIC) in the period 1977-78.

The second data set has 461 cases of computer-related crime which run the gamut from inventory manipulations to hide errors, phony accounting entries to

*Academic institutions, where the primary use of computers tends to be for problem solving, are an exception to this kind of computer application. It is largely this difference in system tasks that is responsible for the fact that intellectual game playing is the dominant form of computer abuse in universities.

cover embezzlements, schemes to penetrate a system and surreptitiously bring about a system crash, to out and out sabotage.

The third data set contains information on quantities of drugs stolen by insiders from drug manufacturers and distributors, the street prices of these drugs, and several related variables for the period 1973-78. The drug-theft data were available only as aggregates and hence no detail was available on individual drug thefts. Consequently, we were unable to provide the same level of statistical and interpretive detail on insider drug theft as we did in the case of the bank fraud and embezzlement data and the computer-related crime data.

Throughout this report we interpret the results of our data analyses in terms of the potential insider threat in the nuclear industry.

DATA SET 1: BANK FRAUDS AND EMBEZZLEMENT

The data on bank fraud and embezzlement (BF&E) cases were made available by the intelligence section of the Federal Deposit Insurance Corporation (FDIC). The data set contains information on bank defalcations of $10,000 or more from January 1, 1976, to December 31, 1977 as reported in FDIC internal reports, Bank Defalcations of $10,000 or More, and FDIC Bank Examination Reports. These data are considerably more detailed than those utilized in our previous report.*

These reports contain information on the position of perpetrators; whether a conspiracy was involved, and, if so, how large; the length of time the incident was concealed; the amount involved (in thousands of dollars); the size of the bank; the bond coverage per incident; and the method of detection. The amount of financial capital involved in an incident is termed the potential loss because in some instances a portion of the loss is recovered.

To determine the relationships between a number of variables which, from both the theoretical and intuitive points of view, must be considered in any analysis of BF&Es, we have proceeded both by estimating equations and by displaying in a series of tables the empirical relationships between variables.

The estimated equations explain the variation in the potential loss variable and in the group size (number of perpetrators) variable. Although a potential loss equation was used in our previous report, this report draws upon a carefully screened subset of the original data set and incorporates information on employee performance bond coverage not previously available. We suspect that, everything else remaining the same, high employee bonds indicate management's awareness of the BF&E potential; therefore, if management is consistent, such awareness should imply better than average internal controls and hence lower average losses.

*J. M. Heineke and Associates, Adversary Modeling: An Analysis of Criminal Activities Analogous to Potential Threats to Nuclear Safeguard Systems, Lawrence Livermore Laboratory, Livermore, Calif., UCRL-13940 (1978).

Our measure of bond coverage is total coverage per incident for the entire bank--which includes the branches in branch banking states. Since our previous study showed that BF&E losses increase with bank size, bond coverage per incident is also likely to increase with bank size; therefore, we have included a measure of bank size in the estimating equation to control for any effects of bank size on bond coverage. The bank size variable is a proxy for the amount at risk or the total exposure of the bank to BF&E. For this reason, predicted losses should increase with bank size.

We have also entered both the number and position of the (highest ranking) perpetrator in the potential loss equation. We expect conspiracy formation to increase potential losses by providing perpetrators freer access to accounts, and consequently, we expect account accessibility, and therefore potential losses, to increase as a function of group size. An important aspect of these relationships is the increasing ability of adversaries to conceal account manipulations as account accessibility increases. The estimated loss equation is:

$$\mathrm{PLOSS} = -\underset{(63.26)}{102.44} + \underset{(14.60)}{35.34}\ \mathrm{PERP} + \underset{(48.15)}{141.91}\ \mathrm{EXEC} + \underset{(55.63)}{86.96}\ \mathrm{TMGT} + \underset{(39.66)}{98.51}\ \mathrm{L/MMGT} \tag{1}$$

$$+ \underset{(4.80)}{9.64}\ \mathrm{SIZE} - \underset{(0.010)}{0.016}\ \mathrm{BOND}$$

$$F(6,272) = 3.68,\ (\Pr > F) = 0.0016,$$

where

PERP = the number of perpetrators (when PERP > 1 a conspiracy is involved),

EXEC = highest ranking perpetrator was executive (bank president or director),

TMGT = highest ranking perpetrator was top management (senior vice presidents, treasurers, trust officers, etc.),

L/MMGT = highest ranking perpetrator was low/middle management (vice presidents, branch managers, assistant cashiers, etc.), SIZE = bank size measured by deposit size, using the ABA deposit group number (see Table 1).

BOND = total employee bond coverage per incident--includes all branches in branch banking states (in thousands of dollars), and

PLOSS = Potential loss--the loss prior to any recoveries from a bank fraud or embezzlement (in thousands of dollars).

TABLE 1. ABA deposit group numbers.

ABA deposit group No.	Bank deposits ($1000)
1	less than 750
2	750-1500
3	1500-2000
4	2000-3000
5	3000-5000
6	5000-7500
7	7500-10,000
8	10,000-15,000
9	15,000-20,000
10	20,000-25,000
11	25,000-35,000
12	35,000-50,000
13	50,000-75,000
14	75,000-100,000
15	100,000-150,000
16	150,000-250,000
17	250,000-500,000
18	500,000-1,000,000
19	1,000,000-2,000,000
20	greater than 2,000,000

Each of the position variables is equal to one when the highest ranking adversary is of that position and is equal to zero otherwise. If EXEC, TMGT and L/MMGT are each zero, the highest ranking perpetrator is a staff member.

The estimated equation bears out our a priori expectations that predicted losses are by far the highest for those of executive rank. Although the parameter estimate for the low/middle management variable is quite precise and larger than that of TMGT, the TMGT is much less precise and statistically is not significantly different from the low/middle management. Hence we conclude that expected losses from executives are much higher than losses from top and low/middle management, which are approximately equal. Expected losses from staff level perpetrators are considerably lower than those for any other group.* Table 2 shows these findings for several cases along with the effects of variation in bank size. The estimated coefficient on bank size is statistically significant† and varies positively with predicted losses. As noted above, bank size is a measure of the amount at risk and hence predicted losses increase with a bank's exposure.

Table 2 also shows that predicted losses per incident are only $3,500 for the case of a small bank with STAFF as perpetrator. For large banks (deposits of one to two billion) this same low level employee averages $138,460 per incident, which is approximately equal to what the president of a small bank averages for a bank fraud or embezzlement. Predicted differences in potential losses as bank size changes are also significant if the perpetrator is an executive, but not as dramatic as for the staff perpetrator. For small banks the predicted potential loss from executives is about $145 thousand while for large banks they average $280 thousand. As far as variation in losses across perpetrator positions for given bank sizes is concerned, Table 2 indicates that the relatively greater account accessibility of bank presidents and the relative autonomy of their actions leads to a higher expected loss from BF&E than for any other group of employees. For example, in an average sized bank,

*A STAFF level perpetrator is the case when EXEC = TMGT = L/MMGT = 0

†Throughout the report all statistical tests on estimated coefficients are conducted with a type I error of size 0.05. Under fairly general conditions, parameter estimates will follow a t distribution. Given the large sample size used in each estimation, a handy conservative rule of thumb is to reject the null hypothesis (the coefficient is zero) when the standard error is less than one half the size of the estimated coefficient for two tail tests, and six-tenths the size of the estimated coefficient for one tail test.

TABLE 2. Predicted losses, perpetrator position, and bank size.[a]

Predicted loss ($1000)	Highest ranking perpetrator	Bank size[b] and ABA No.
145.14	EXEC	Small (5)
96.24	MGT[c]	Small (5)
3.50	STAFF	Small (5)
203.25	EXEC	Average (11)
154.08	MGT[c]	Average (11)
61.34	STAFF	Average (11)
280.37	EXEC	Large (19)
231.20	MGT[c]	Large (19)
138.46	STAFF	Large (19)

[a] Losses are calculated for the case in which the number of perpetrators is one and when BOND = $1400 (the sample mean).

[b] Bank sizes are defined as:
small = $3-5 million in deposits
average = $25-35 million in deposits
large = $1-2 billion in deposits.

[c] Since the coefficients TMGT and L/MMGT were not statistically different, we use MGT to represent all management and have used the mean value of these two coefficients as the coefficient of MGT.

predicted potential losses for bank presidents (executives) is $203 thousand while predicted losses average $154 thousand for managers and only $61 thousand for staff members.

Table 3 shows the relationship between the potential loss, the number of perpetrators, and bank size for several values of these variables and highlights the substantial impact conspiracy size has upon predicted BF&E losses. For an average size bank ($25-35 million in deposits) predicted losses increase from $203 thousand to $238 thousand per incident by going from a single adversary to a conspiracy involving two persons. The move from a two person to a five person conspiracy further increases predicted losses to $344 thousand. Obviously the increasing returns to group size will not last indefinitely; note also that the onset of decreasing returns to group size can not be detected in a linear regression equation. But since conspiracy size in our sample ranges from one to nineteen, it is safe to assume that these large

TABLE 3. Predicted losses, the number of perpetrators, and bank size.

Predicted loss[a] ($1000)	Number of perpetrators	Bank size[b] and ABA No.
145.41	1	Small (5)
180.75	2 (sample mean)	Small (5)
286.77	5	Small (5)
203.25	1	Average (11)
238.59	2	Average (11)
344.61	5	Average (11)
280.37	1	Large (19)
315.71	2	Large (19)
421.73	5	Large (19)

[a] Losses are calculated for the case in which the number of perpetrators is one and when BOND = $1400 (the sample mean).

[b] Bank sizes are defined as: small = $3-5 million in deposits
average = $25-35 million in deposits
large = $1-2 billion in deposits.

payoffs to expanding group size are operative at least up to groups of size four or five. Equation (1) and Table 3 indicate that the marginal impact on adversary gains of adding an additional individual to a conspiracy is estimated to average about $35,000.

Table 4 shows predicted BF&E losses against low, mean and high employee bond averages for the cases of small, average and large banks. Although the estimated coefficient of BOND is not as precise as one would like, there is little doubt that BOND has a negative impact on losses. This is consistent with the hypothesis that the amount of employee bond coverage could be used as an indicator of management's awareness of the insider BF&E and hence also as an indicator of the attention given to internal controls. For example, in an average size bank, an increase in bond coverage incident from $125,000 to

TABLE 4. Predicted losses, employee bond coverage, and bank size.

Predicted loss[a] ($1000)	Bond coverage	Bank size and ABA No.
121.01	Low ($125k)	Small (5)
102.01	Mean ($1400k)	Small (5)
43.01	High ($5000k;	Small (5)
178.85	Low ($125k)	Average (11)
159.85	Mean ($1400k)	Average (11)
100.85	High ($5000k)	Average (11)
255.97	Low ($125k)	Large (19)
236.97	Mean ($1400k)	Large (19)
177.97	High ($5000k)	Large (19)

[a] Losses are calculated for the case in which the number of perpetrators is one and when BOND = $1400 (the sample mean).

$1,400,000 (the sample mean) reduces predicted BF&E losses from $178 thousand to $159 thousand. A further increase in coverage to $5 million per incident reduces expected losses, on average, an additional $59 thousand. Again, it is not the bond coverage *per se* that is responsible for lower BF&E losses, but rather the awareness of managers to the general BF&E problem which in turn results in higher bonds, tighter control, and consequently lower loss size per incident.

The discussion in this section indicates that indirect methods may be useful to regulators in checking for adherence to regulatory code: namely, if a variable can be identified that is highly correlated with a desired activity (e.g., employee bond coverage and tight internal controls) then observing the deviation of this variable from, say, the industry mean, will provide an indirect check on the level of the desired activity. We also found that the higher the position of the adversary, the larger the conspiracy and the larger the bank, *ceteris paribus*, the higher are expected BF&E losses. Finally, note that the F statistic reported after Eq. (1) means that the estimated PLOSS equation is significant at the 0.0016 level. Roughly, this indicates that we may be quite certain that the variables entering this equation are in fact related to PLOSS.

We used the same set of variables to try to explain the variation in the size of the adversary group over the sample. In general, what lies behind the size of a conspiracy? Why are some larger than others? We did not attempt to provide a behavioral explanation for these questions, but sought a set of variables which statistically explained movements in PERP over the sample. To this end we noted that the larger the targeted BF&E, the more individuals (on average) were needed to circumvent controls. When an executive is involved in an incident, the average number of perpetrators is larger. Evidence of the loss size-to-number of perpetrators relationship is contained in the PLOSS equation, while the latter effect seems to stem primarily from the fact that executives tend to target large BF&Es which require more cooperation, *ceteris paribus*, and also from the fact that executives are in a unique position to encourage cooperation from underlings. One other reason we would expect a larger than average number of perpetrators to be involved when a bank president is involved is that a bank president, unlike top management, usually will not have direct control over accounts in the various departments and hence will often seek the cooperation of others when continuing account access is needed.

Other than potential losses (PLOSS) and whether or not the perpetrator was an executive (EXEC), we would also expect to find employee bond coverage to be positively related to the number of perpetrators. This follows from our argument above that bond coverage is a proxy for managerial awareness of the insider problem and hence will be closely correlated with the extent or effectiveness of internal controls. Also, it is reasonable to expect that the more effective the controls, the greater the need for cooperation and hence, *ceteris paribus*, the larger the conspiracy. The propositions are born out in the following regression equation:

$$\begin{array}{llllll} \text{PERP} = & 1.150 & + 0.0006\ \text{PLOSS} & + 0.7624\ \text{EXEC} & + 0.00011\ \text{BOND} & \quad (2) \\ & (0.094) & (0.0002) & (0.1415) & (0.00003) & \end{array}$$

$$F = (3,272) = 14.66,\ (Pr > F) > 0.0001.$$

Each coefficient in the estimated equation has a statistically significant* and positive impact on conspiracy size. Banks with large employee bonds, incidents with large losses, and incidents involving executives all tend to be associated with a larger than average number of perpetrators. We conclude that for financially motivated crimes in general, incidents involving large losses and incidents involving executives are likely to be characterized by conspiracies. Also the more effective the controls the more likely it will be that a conspiracy will be necessary if an attempt is to be made. Presumably this implies that the total number of attempts will fall with increased controls, as potential adversaries either decide the gain is no longer worth the risk or are forced to form conspiracies to keep probabilities of success acceptably high. An interesting question is whether failure probabilities are significantly different for conspiracies than for single perpetrators.† This question must be addressed if one is to intelligently assess the implications of policies designed to increase internal security.

Several distinctions and insights which were gained from conversations with FDIC examiners are reviewed before proceeding to a series of tables in which relationships between pairs of variables are explored in a matrix format.

First, the regularity of FDIC bank examinations depends upon historical experiences with a bank. If a bank has been historically sound and well managed with adequate internal controls, examinations may be scheduled as infrequently as once in an eighteen month cycle--which could conceivably mean only once in 36 months. The scope of examinations also depends upon the historical record. Historically sound banks might be examined only on one or two accounts, while a bank with traditionally weak controls will receive a full examination during each visit.

Second, the FDIC attempts to make unannounced examinations, but in some cases, e.g., if a computer service bureau is handling one or more of a bank's accounts, the bureau may be notified a day in advance to insure the requisite information is available to begin the examination.

*That is, the null hypothesis that the coefficient is zero is rejected for each estimate at the 0.05 level of significance. See footnote† page 6.

†The next section of this report, Computer-Related Crime, estimates failure probabilities to be approximately 25% higher for computer-related crimes involving conspiracies than for those involving a single perpetrator.

Third, the data set contains information on suspects, not on convicted perpetrators. FDIC investigators claim that virtually all suspects are guilty. Examiners tend to be cautious and do not use suspect names in reports unless the evidence is overwhelming. If we used only cases involving convicted suspects, the sample size would drop to but a few points. We were told that the reasons for this are:

a. Prejudice against white collar crimes by law enforcement officials and hence an unwillingness to allocate necessary resources to build strong cases.

b. Law enforcement officials who do bring cases often do not sufficiently understand the accounting intricacies to prepare a strong case--even though the case is open and shut as far as examiners are concerned.

c. Jurors in BF&E cases are not banking executives or a panel of peers, but men and women off the street who seldom understand the machinations involved. Hence, reasonable doubt often translates into acquittal but for the wrong reasons.

d. Points a., b., and c. lead to high acquittal rates and hence a fear on the part of bankers that a libel suit for damages from a false accusation, defamation of character etc., will be filed. Bankers often find it safer to take the loss and learn.

The upshot of this discussion is that even if most perpetrators are detected, few are convicted; this provides a strong incentive for some individuals to view BF&E almost as an occupation. Indeed a number of major embezzlers have found bank employment again and again under various guises and reap a fairly steady, high income from their activity. Of fundamental consideration to authorities charged with securing nuclear facilities is that every possible effort must be made to insure conviction of guilty adversaries and not to just rest on the knowledge that "we got him." Low conviction rates have very undesirable incentive effects.

Bank examinations are performed by external regulatory agencies--state or federal bank examiners. Audits, as used here, are internal management directed audits. In large banks, these are usually done on an ongoing basis by an internal auditing unit, while in small banks an external accounting firm is likely to be called upon to conduct periodic audits. In substance, audits and examinations amount to the same thing.

We now turn to the tables. These tables are straightforward in their interpretation and we, therefore, comment only upon a select few. The reader should keep in mind that the tables are based upon our sample of BF&E cases with the exact number of observations given in a footnote following each table.*

Tables 5-7 display information related to perpetrator positions.

Table 6 gives the distribution of detection methods, given the position of the highest ranking perpetrator. Note that executives and top management are more likely to be caught via bank examinations (this is especially true of executives) than via internal audits, while low/middle management and staff are much more likely to be detected in an internal audit than by a bank examiner. This observation dramatically points up the lack of independence between internal auditors and the top officials of the bank--a situation well known and emphasized by the federal bank examiners we have spoken with: It is very difficult for an auditor to objectively audit accounting entries made by his or her boss. The analogy to the nuclear industry is obvious. Great care must be taken to insure that inspectors are truly independent, in the sense that their position or livelihood could in no way be affected by an adverse report concerning the operation of a plant. Also notice that branch managers are detected far more often by internal audit than by examination--an observation that reinforces the point being made here. In the case of branch managers, an audit is done by the parent bank which has all the proper incentives for uncovering a defalcation. Next notice that, for obvious reasons, confessions are most likely from lowest level perpetrators and least likely from highest level perpetrators. Finally, since the amount of interaction with the public decreases the higher the position, we see that outsiders are most likely to aid in the detection of staffers and least likely to aid in the detection of a bank president.

On a related point, we computed an estimate of the probability that a branch manager will attempt a BF&E since, of all managment positions in a bank, branch managers offer the closest analog to managers of a nuclear facility. This probability was estimated by dividing the total number of FDIC

*The number of observations used in computing table entries varies from table to table. This arises from less than complete information on each of the variables of interest. Therefore, each table uses the maximum number of data points containing observations on each variable. The tables are grouped together at the end of the section.

regulated bank branch managers involved in a BF&E (either as the sole perpetrator or as a member of a conspiracy) by tne total number of branches in FDIC regulated banks in the period 1976-77. That ratio is 0.0020, with the interpretation that over the 1976-77 time period, if one were to choose a branch bank at random, there would be approximately two chances in one thousand that the manager would turn out to be an embezzler. The estimate arrived at in this manner understates the true probability since a few branches will in fact be automated teller machines. Hence, our data indicates that more than two of every thousand managers are engaged in embezzlement.

The first column of Table 8 illustrates one of the findings of Eq. (2): viz., that executives are far more likely to be involved in a conspiracy than employees at any other level. In our sample, a full 71% of the cases involving executives involved more than one perpetrator. Some of the reasons for this phenomenon were discussed following Eq. (1). Table 9 supports the estimated PERP equation and shows that not only are executives likely to be involved in conspiracies, but that the average size of the conspiracy is larger for executives.

Tables 10 and 11 continue to focus on group size. Table 11 shows that bank examinations are not an effective method of detection when five or more conspirators are operating; this presumably reflects the fact that large groups working together can usually effectively disguise account manipulations, at least during the rather short visits of examiners. Also in Table 11 confessions point up the rather obvious Achilles heel of large conspiracies, viz., that "all men are not of the same fiber"; as group size grows it becomes increasingly likely that an individual who has much less ability to withstand the tensions associated with the cat and mouse game of endless accounting coverups will become involved with the group. Confessions in large conspiracies are approximately twice as likely as in any other group.

Tables 12-14 give the distribution of potential losses from BF&E. Much of the information in these tables is reflected by the two estimated equations, Eq. (1) and Eq. (2), we presented above. One observation not brought out in the equations is the role of top management in BF&E cases; Table 13 shows that from any given size of loss, top management appears to have very low involvement in BF&E. There are several reasons for this unexpected finding. First, when executives are in collusion with others (which is often), the most likely participants are top managers. But because we record only the position of the highest ranking perpetrator in conspiracies, the role of top managers in these conspiracies is hidden. Second, the ranks of top management, according to industry sources, are much less likely to contain disgruntled employees than the ranks of low/middle management. In addition, salary levels in banking are notoriously low until top management and executive positions are reached. This situation provides a further incentive for a disgruntled low/middle manager to consider BF&E which may not be there for more highly paid disgruntled top managers.

Tables 15 and 16 examine the relationship between the length of time a loss is concealed prior to its discovery and the position of the perpetrator. Table 16 shows that executives are not, on average, able to conceal BF&Es as long as other managers. This apparent anomaly possibly results from differences in the thoroughness of auditing procedures as a function of the position of the individuals responsible for the transaction(s) or account(s). More specifically, federal bank examiners often examine the transactions of executives much more carefully than those of other managers. This policy arises from the relative autonomy of bank presidents (and directors) and hence their relative immunity from regular internal controls. (This point also arose in our discussion of Table 6.)

Finally, Tables 17-19 are marginal distributions on detection frequencies by method of detection, on the type of group--given a conspiracy was formed--and on the size of conspiracies. We find that bank examinations, audits, and confessions are equally effective methods of discovery. That examinations and audits are effective means of rooting out defalcations is, of course, not surprising; but the fact that confessions are equally important may be of interest in other regulated industries. For example, NRC might want to study policy alternatives which would encourage confessions. This may be especially practical in conspiracies since confessions are the dominant means of discovery in large conspiracies (see Table 11).

Table 20 gives summary information on 59 Hobbs Act cases involving extortion threats received by FDIC regulated banks over the period 1975-78. Although there were more than 59 cases in this time period, our sample includes only those mistakenly reported to FDIC.* Hence, we are not sure of the nature of biases, if any, which may distort conclusions drawn from this

*Although banks are required to report BF&E cases to the FDIC, there is no requirement of this type for Hobbs Act cases or extortion threats.

sample. Since Hobbs Act incidents involve using hostages to extort demands and the analog in the nuclear industry seems to be a realistic scenario, we felt some information is better than none and decided to include Table 20. The extortion threats reported in the table are primarily bomb threats and a few death threats which were used in attempts to extort payments from banks. As the table indicates, only 14% of the incidents actually resulted in a financial loss to the victim, but in none of these cases was the perpetrator apprehended. So at least in this sample, once the adversary gains possession of the ransom, it is highly likely it will remain in his possession.

TABLE 5. Joint distribution of perpetrator position and method of detection: BF&E cases, 1976-77.[a]

	Method of detection[c]					
Perpetrator position[b]	Bank examination	Internal audit	Outsider information	Insider information	Confession	Absence
Executive	0.121	0.058	0.018	0.033	0.058	0.003
Top management	0.033	0.025	0.011	0.014	0.025	0.003
Low/middle management	0.044	0.121	0.018	0.066	0.125	0.003
Staff	0.022	0.062	0	0.040	0.084	0.003
Branch manager	0.007	0.029	0.007	0.007	0.018	0

[a] Total number of cases with data on each variable is 292. Rounding errors may cause totals to deviate from one.

[b] First four positions are mutually exclusive and exhaustive. Conspiracy cases list the position of the highest ranking perpetrator. The category branch manager stands alone and is reported whether or not the branch manager was the highest ranking perpetrator.

[c] See Abbreviations and Definitions.

TABLE 6. Distribution of method of detection, conditional on perpetrator position: BF&E cases, 1976-77.[a]

Given that	Distribution of method of detection[c] is:					
perpetrator position[b] is:	Bank examination	Audit	Outsider information	Insider information	Confession	Absence
Executive	0.41	0.20	0.11	0.06	0.20	0.01
Top management	0.29	0.23	0.13	0.10	0.23	0.03
Low/middle management	0.12	0.32	0.17	0.05	0.33	0.01
Staff	0.10	0.29	0.19	0	0.40	0.02
Branch manager	0.11	0.42	0.11	0.11	0.26	0

[a] Total number of cases with data on each variable is 272. Rounding errors may cause totals to deviate from one.

[b] First four positions are mutually exclusive and exhaustive. Conspiracy cases list the position of the highest ranking perpetrator. The category branch manager stands alone and is reported whether or not the branch manager was the highest ranking perpetrator.

[c] See Abbreviations and Definitions.

TABLE 7. Distribution of bank fraud and embezzlement cases by perpetrator position: 1976-77.[a]

Perpetrator position[b]	Probability
Executive	0.30
Top management	0.12
Low/middle management	0.29
Staff	0.21
Branch manager	0.08

[a] Total number of cases with data on each variable is 286. Rounding errors may cause totals to deviate slightly from one.

[b] First four positions are mutually exclusive and exhaustive. Conspiracy cases list the position of the highest ranking perpetrator. The category branch manager stands alone and is reported whether or not branch manager was the highest ranking perpetrator.

TABLE 8. Distribution of collusive attacks on banks, conditional on perpetrator position: BF&E cases, 1976-77.[a]

Given that perpetrator position[b] is:	Probability
Executive	0.71
Top management	0.18
Low/middle management	0.30
Staff	0.14
Branch manager	0.28

[a] Total number of cases with data on each variable is 286. Rounding error may cause totals to deviate slightly from one.

[b] First four positions are mutually exclusive and exhaustive. Conspiracy cases list the position of the highest ranking perpetrator. The category branch manager stands alone and is reported whether or not branch manager was the highest ranking perpetrator.

TABLE 9. Distribution of conspiracy size, conditional on perpetrator position: BF&E cases, 1976-77.[a]

Given that perpetrator positi[b] is:	Distribution of number of perpetrators is:				
	1	2	3	4	5 or more
Executive	0.29	0.38	0.15	0.07	0.11
Top management	0.82	0.06	0.09	0	0.03
Low/middle management	0.70	0.16	0.09	0.04	0.01
Staff	0.86	0.09	0.02	0	0.03
Branch manager	0.7	0.05	0.15	0.1	0

[a]Total number of cases with data on each variable is 286. Rounding errors may cause totals to deviate slightly from one.

[b]First four positions are mutually exclusive and exhaustive. Conspiracy cases list the position of the highest ranking perpetrator. The category branch manager stands alone and is reported whether or not branch manager was the highest ranking perpetrator.

TABLE 10. Distribution of number of perpetrators, conditional on bank size: BF&E cases, 1976-77.[a]

Given that bank size[b] is:	Distribution of number of perpetrators is:				
	1	2	3	4	5 or more
Small	0.57	0.27	0.11	0.05	0
Medium	0.65	0.2	0.07	0.03	0.04
Large	0.65	0.12	0.11	0.03	0.09

[a]Total number of cases with data on each variable is 284. Rounding errors may cause totals to deviate from one.

[b]Bank size is defined as follows:
small = up to $10,000,000 in deposits
medium = $10,000,000-$100,000,000 in deposits
large = over $100,000,000 in deposits.

TABLE 11. Distribution of method of detection, conditional on number of perpetrators: BF&E cases, 1976-77.[a]

Given that number of perpetrators is:	Distribution of method of detection is[b]:					
	Bank examination	Internal audit	Outsider information	Insider information	Confession	Absence
1	0.17	0.30	0.05	0.18	0.29	0.01
2	0.24	0.28	0.05	0.1	0.29	0.03
3	0.37	0.19	0.07	0.15	0.22	0
4	0.45	0.09	0.09	0.09	0.27	0
5 or more	0.15	0.31	0	0.08	0.46	0

[a] Total number of cases with data on each variable is 274. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

TABLE 12. Distribution of loss, conditional on bank size: BF&E cases, 1976-77.[a]

Given that bank size[c] is:	Distribution of potential loss[b] is:					
	0-49	50-99	100-199	200-499	500-999	1000 and over
Small	0.515	0.151	0.166	0.106	0.045	0.015
Medium	0.569	0.145	0.104	0.090	0.048	0.041
Large	0.600	0.160	0.106	0.053	0.053	0.026

[a] Total number of cases with data on each variable is 285. Rounding errors may cause totals to deviate from one.

[b] Potential loss is total loss to bank exclusive of any recovery and is measured in thousands of dollars.

[c] Bank size is defined as follows:
small = up to $10,000,000 in deposits
medium = $10,000,000-$100,000,000 in deposits
large = over $100,000,000 in deposits.

TABLE 13. Distribution of perpetrator position, conditional on loss size: BF&E cases, 1976-77.[a]

Given that potential loss[b] is:	Distribution of perpetrator position[c] is:				
	Executive	Top management	Low/middle management	Staff	Branch manager
0-49	0.20	0.1	0.39	0.31	0.08
50-99	0.37	0.12	0.42	0.09	0.05
100-199	0.5	0.15	0.29	0.06	0.09
200-499	0.39	0.17	0.35	0.09	0.09
500-999	0.36	0.14	0.5	0	0
1000 and over	0.56	0	0.44	0	0.11

[a] Total number of cases with data on each variable is 286. Rounding errors may cause totals to deviate from one.

[b] Potential loss is total loss to bank exclusive of any recovery and is measured in thousands of dollars.

[c] First four positions are mutually exclusive and exhaustive. Conspiracy cases list the position of the highest ranking perpetrator. The category branch manager stands alone and is reported whether or not the branch manager was the highest ranking perpetrator.

TABLE 14. Distribution of loss size, conditional on perpetrator position: BF&E cases, 1976-77.[a]

Given that perpetrator	Distribution of potential loss[c] is:					
position[b] is:	0-49	50-99	100-199	200-499	500-1000	1000 and over
Executive	0.39	0.19	0.2	0.11	0.06	0.06
Top management	0.5	0.16	0.16	0.13	0.06	0
Low/middle management	0.58	0.16	0.09	0.07	0.06	0.04
Staff	0.86	0.07	0.03	0.03	0	0
Branch manager	0.62	0.1	0.14	0.1	0	0.05

[a] Total number of cases with data on each variable is 286. Rounding errors may cause totals to deviate from one.

[b] First four positions are mutually exclusive and exhaustive. Conspiracy cases list the position of the highest ranking perpetrator. The category branch manager stands alone and is reported whether or not the branch manager was the highest ranking perpetrator.

[c] Potential loss is total loss to bank exclusive of any recovery and is measured in thousands of dollars.

TABLE 15. Distribution of perpetrator position, conditional on time concealed: BF&E cases, 1976-77.[a]

Given that time concealed[b] is:	Distribution of perpetrator position[c] is:				
	Executive	Top management	Low/middle management	Staff	Branch manager
Short	0.22	0.12	0.28	0.38	0.1
Medium	0.54	0.07	0.26	0.12	0.05
Long	0.34	0.14	0.41	0.1	0.07

[a] Total number of cases with data on each variable is 136. Rounding errors may cause totals to deviate from one.

[b] Time concealed is the total length of time activity is concealed and is measured as follows: Short = 0-6 months
medium = 7-24 months
long = over 25 months.

[c] First four positions are mutually exclusive and exhaustive. Conspiracy cases list the position of the highest ranking perpetrator. The category branch manager stands alone and is reported whether or not the branch manager was the highest ranking perpetrator.

TABLE 16. Distribution of time concealed, conditional on perpetrator position: BF&E cases, 1976-77.[a]

Given that perpetrator position[b] is:	Distribution of time concealed[c] is:		
	Short	Medium	Long
Executive	0.21	0.60	0.19
Top management	0.43	0.29	0.29
Low/middle management	0.34	0.37	0.29
Staff	0.66	0.24	0.1
Branch manager	0.5	0.3	0.2

[a] Total number of cases with data on each variable is 136. Rounding errors may cause totals to deviate from one.

[b] First four positions are mutually exclusive and exhaustive. Conspiracy cases list the position of the highest ranking perpetrator. The category branch manager stands alone and is reported whether or not the branch manager was the highest ranking perpetrator.

[c] Time concealed is the total length of time activity is concealed and is measured as follows:

Short = 0-6 months
medium = 7-24 months
long = over 25 months.

TABLE 17. Frequency of detection by method.[a]

Method of detection	Probability
Bank examination	0.25
Audit	0.26
Insider information	0.05
Outsider information	0.14
Confession	0.28
Absence	0.01

[a]Total number of cases with data on method of detection is 295.

TABLE 18. Distribution of perpetrators by type of group: BF&E cases, 1976-77.[a]

Perpetrator group	Probability
Single perpetrator	0.61
Insider with other insider(s)	0.18
Insider with outsider(s)	0.21

[a]Total number of cases is 296.

TABLE 19. Distribution of group size: BF&E cases, 1976-77.[a]

Number of perpetrators	Probability
1	0.61
2	0.21
3	0.10
4	0.03
5 or more	0.04

[a]Total number of cases is 274.

TABLE 20. Summary of Hobbs Act violations and extortion threats against banks as reported to FDIC: 1975-78.[a]

Total number of case reported: 59

Proportion of cases in which loss was incurred: 0.14

Average loss: $18,244

Proportion of cases in which an arrest was made (includes hoaxes): 0.20

Proportion of cases which were hoaxes: 0.25[b]

Average amount demanded (including hoaxes): $2,537,450[c]

Proportion of bomb threats: 0.24[b]

Proportion of bomb threat hoaxes: 0.10[b]

Proportion of kidnappings: 0.24

Proportion of kidnap attempts or threats: 0.08[b]

Proportion of kidnap threat hoaxes: 0.12[b]

Proportion of death threats: 0.02[b]

Proportion of death threat hoaxes: 0.02[b]

Proportion of cases in which origin of extraction threat was:

a. note or letter: 0.03

b. phone call: 0.20

c. unknown: 0.77

(Of the 59 cases reported, in only eight cases did money pass from the victim to the adversary. No arrest was made in any of these cases.)

[a] Banks are not required to report Hobbs Act cases to the FDIC. Hence these cases are a subset of all Hobbs Act cases that occurred in this time period--cases which were (mistakenly) reported to FDIC.

[b] We have differentiated "threats" and "threat hoaxes" according to the credibility of the threat as detailed in the FDIC reports.

[c] In one case $50,000,000 was demanded. If this case is omitted, the average demand is $39,420.

DATA SET 2: COMPUTER-RELATED CRIME

The data subjected to analysis in this section were obtained from the files of Donn Parker of SRI International. The information on the date and type of computer crime, the type of organization identified as the principal victim, the size of the loss due to the crime, the number of perpetrators, the position of the perpetrator or highest ranking perpetrator if a conspiracy is involved, the location of the perpetrator(s)--insider(s) or outsider(s), and limited information on the disposition of individual cases were drawn from 461 computer-related crime incidents for the period 1958-78.

Although computer crimes with immediate monetary payoffs have been the most common type of abuse in the past, losses of information or other negotiable property via computer penetration are more of a threat to intelligence agencies, the nuclear industry, and other highly specialized organizations. A number of computer crimes outside the nuclear industry have immediate relevance as analogs of potential threats to the industry. Incidents as diverse as inventory manipulation schemes used to disguise thefts, to "salami-tactics" where amounts of money small enough to be viewed as statistical discrepancies are continuously diverted until many thousands of dollars are collected, to the use of "trojan horse" programs* to erase data and either gain control over an operating system or to crash an operating system are obvious examples. Detailed case descriptions of such events are readily available in the popular press. The objective here is to investigate, via a series of tables and an estimated equation, the relationship between certain variables which appear to be important factors in computer-related crimes. An estimated equation explores the relationship between computer crime losses and the position of perpetrators, the type of victim, the number of perpetrators, and a shift variable that indicates whether or not outsiders were involved in the incident.

*A program is clandestinely placed in the operating system, which, on a certain combination of events goes into operation. The results of such an attack depend upon the program. But to some extent or another the system ends up under the control of the adversary.

In perusing the estimated equation and tables in this section, keep in mind that the data include only those incidents which have been discovered. There is complete agreement among those familiar with white-collar crime and computer-related crime in particular, that by far the greater number of cases go undetected. The standard estimate is that only about 15% of all cases are discovered. Since less competent perpetrators tend to be discovered, the data contains biases imparted by this fact. For example, if on he average computer employees are brighter or more competent than noncomputer employees, then, ceteris paribus, estimates of the distribution of perpetrators over the type of perpetrator will contain a downward bias for computer personnel. Of course, the same statement is true for executives and other types of employees as well as for the various types of victim institutions. If, for example, computer service bureaus tend to require on average a more intelligent employee than do, say, government agencies, then, ceteris paribus, the same downward bias would appear for computer service bureaus in the distribution of cases over victim institutions. Similar arguments hold if it is easier to detect incidents in some jobs or some industries than in others merely because of the nature of the job or industry.

Regression analysis was used to estimate the following equation relating computer crime loss size (in thousands of dollars) to the variables listed above:

$$\begin{aligned} \mathrm{LOSS} = {} & \underset{(1431.44)}{9032.65} + \underset{(61.14)}{170.67}\mathrm{PERP} - \underset{(626.34)}{1151.57}\mathrm{OUTSIDER} \\ & + \underset{(687.68)}{1319.67}\mathrm{EXEC} - \underset{(1548.34)}{9213,39}\mathrm{SALMFC} \\ & - \underset{(1415.69)}{9044.82}\mathrm{FIN} - \underset{(1533.91)}{8943.19}\mathrm{GOVT} - \underset{(4031.01)}{10631.87}\mathrm{MED} \\ & - \underset{(1778.02)}{8579.33}\mathrm{COMPSERV} - \underset{(4032.17)}{6544.68}\mathrm{COMPUB} \\ & + \underset{(3971.12)}{197{,}408.83}\mathrm{CORP} \end{aligned} \tag{3}$$

$$F(10,174) = 235.58, \quad (Pr > F) > 0.0001$$

The number of observations used in the regression and the reported F statistic indicate beyond any reasonable doubt that the variables included in the estimated equation are important determinants of computer crime losses.* This equation is the basis of the information presented in Tables 21-23, in which predicted computer crime losses are displayed for various combinations of the determinants of these losses. Each calculation presents cases in which a corporation was not the perpetrator. We have done this due to the existence of a few very large losses inflicted by corporations which are far above mean losses and which tend to impart a strong upward bias to predicted losses in cases in which a corporation is the perpetrator.

Table 21 presents predicted losses as a function of the number and type of perpetrator. In particular, predicted losses for the case when an executive is the sole perpetrator are contrasted with the case in which any other insider acting alone is the perpetrator. These two numbers are $1,478,180 and $158,510 respectively.† When the perpetrator is an executive acting alone, predicted losses are over nine times larger than when the perpetrator is any other insider acting alone. Notice that predicted losses are systematically higher when an executive is involved no matter how many individuals may be involved in the conspiracy and that predicted losses increase in conspiracy size. This supports the findings of our earlier study in which bank embezzlement data showed executives to be far the greatest threat to the financial security of banks.** If anything, computer-related crime cases imply that officials at the top of victim organizations are even more of a threat than indicated by the banking industry data.

*Information was available on 461 incidents yet only 174 observations were used to estimate Eq. (3). This was because individual accounts of incidents invariably do not have complete information on each of the variables defined in the estimated equation. The 174 incidents contained information on the variables included in Eq. (3).

†Calculations were carried out for the case in which a financial institution is the victim.

**See J. M. Heineke and Associates, Adversary Modeling: An Analysis of Criminal Activities Analogous to Potential Threats to Nuclear Safeguard Systems, Lawrence Livermore Laboratory, Livermore, Calif., UCRL-13940 (1978) and the previous section of this report.

TABLE 21. Predicted losses and the number and type of perpetrator.

Predicted loss per incident ($1000)[a]	Number of perpetrators[b]	Type of perpetrator
1478.18	1	Executive
1734.19	2.5 (mean)	Executive
2160.90	5	Executive
3014.30	10	Executive
158.51	1	All other[c]
414.53	2.5 (mean)	All other
841.23	5	All other
1694.63	10	All other

[a] Losses are calculated for the case in which the victim is a financial institution.

[b] The number of perpetrators varies between 1 and 60 in the sample.

[c] All other indicates that the highest ranking perpetrator(s) is/are below the rank of executive and includes cases in which the perpetrator is unknown but excludes cases in which a corporation is the perpetrator.

For example, if an executive is the perpetrator, predicted losses more than double from when the executive acts alone to when the executive either leads or is involved in a large conspiracy with ten members.

Table 22 shows that predicted losses are highest in computer service companies and lowest in communications and publications, the former being over four times larger than the latter. One suspects that this reflects, more than any other single factor, differences in opportunities confronting employees in these industries. Educational institution losses are also quite high but these losses tend to be computer time losses from unauthorized accesses. Each of these cases indicates that the existence of opportunities and groups of bright individuals often leads to a system penetration. For the case of computer service companies, adversary motivation is predominately financial, while for educational institutions one suspects that intellectual game playing by system hackers is the predominate goal. Either case if transplanted to the nuclear industry, would be of serious concern. Tables 21-23 support our findings concerning the magnitude of the threat posed by very top management.

TABLE 22. Predicted losses, victim institution, and type of perpetrator.

Predicted loss ($1000)[a]	Victim institution	Type of perpetrator[b]
2623.28	Finance	Executive
2797.85	Government	Executive
2899.48	Medical	Executive
3080.40	Educational	Executive
2723.72	Sales and manufacturing	Executive
1210.79	Communication and publications	Executive
3263.34	Transportation and utilities	Executive
5297.99	Computer service	Executive
1303.61	Finance	All other
1478.18	Government	All other
1579.81	Medical	All other
1760.73	Educational	All other
1404.05	Sales and manufacturing	All other
0[c]	Communications and publications	All other
1943.67	Transportation and utilities	All other
3978.32	Computer service	All other

[a] Losses are calculated for the case where the number of perpetrators equals one.

[b] Executive is highest ranking perpetrator. All other indicates that the highest ranking perpetrator(s) is/are below the rank of executive and includes cases in which the perpetrator is unknown.

[c] Predicted loss here is slightly negative, but statistically not different from zero.

Table 23 shows predicted losses as a function of whether the incident involves conspiracy, and if so, how large and the position of the highest ranking perpetrator. The interesting information here is not only that collusion among adversaries pays off (as we saw earlier in Table 21) but that expected losses when an outsider is involved (either acting alone, with other outsiders or with insiders) are consistently less than when only insiders are involved. Clearly outsiders are responsible for or partly responsible for substantial losses, but the estimated equation indicates the more serious threat is posed by an insider or group of insiders.

Table 24 lists a series of probability calculations based upon the computer crime data set. Each entry in the table indicates the size of the subsample which was available for the calculation. In general, the probability of success conditional on some factor α was estimated by dividing the number of cases characterized by factor α, in which the perpetrator was not apprehended, by the total number of cases characterized by α on which case disposition information was available--information on whether or not the perpetrator was apprehended. For example, the estimated probability of success given an executive was involved is 0.022 (note entry c), and was obtained by dividing the number of successful cases involving executives (one) by the total number of cases involving executives in which disposition information was available (45).

Entries a and b in the table compare success probabilities of single perpetrators relative to those for conspiracies. The data set indicates conspiracies have approximately a 25% higher failure rate than do incidents involving single perpetrators. Several possible explanations for this finding were discussed above in connection with the bank fraud data.

Entries c-f show that computer employees have higher estimated success probabilities than do other categories of employees. In fact, this probability is 460% higher than that for EXEC, the smallest success probability of the group. Of course, we expect, ceteris paribus, that perpetrators with the more applicable skills will be most successful. The number of observations available for each of these calculations is reasonably large except for the case of ex-employees.

Entries g-k tend to support the conclusion that physical destruction of hardware and/or software is relatively more difficult to trace than are other types of crimes, although the number of sample points available for several of

TABLE 23. Predicted losses, outside involvement, number and type of perpetrator.

Predicted loss($1000)[a]	Outsider involvement	Conspiracy	Type of perpetrator
9371.43	Yes	No (Number of perp = 1)	Executive
10522.99	No	No (Number of perp = 1)	Executive
9627.45	Yes	Yes (Number of perp = mean)	Executive
10779.02	No	Yes (Number of perp = mean)	Executive
10054.15	Yes	Yes (Number of perp = 5)	Executive
11205.72	No	Yes (Number of perp = 5)	Executive
8051.76	Yes	No (Number of perp = 1)	All other[b]
9203.33	No	No (Number of perp = 1)	All other
8307.78	Yes	Yes (Number of perp = mean)	All other
9459.35	No	Yes (Number of perp = mean)	All other
8734.48	Yes	Yes (Number of perp = 5)	All other
9203.33	No	Yes (Number of perp = 5)	All other

[a] Losses are calculated for case when victim is financial institution.

[b] All other indicates that the highest ranking perpetrator(s) is/are below the rank of executive and includes cases in which perpetrator(s) is/are unknown.

TABLE 24. Estimated probabilities of success: reported cases.

Entry	Estimated Probabilities	Given	Size of subsample used in calculations
a	0.115	A single perpetrator	156
b	0.092	A conspiracy	141
c	0.022	EXEC is involved	45
d	0.125	CEMP is involved	56
e	0.074	NCEMP is involved	54
f	0.083	EXEMP is involved	12
g	0.304	Crime is PHYSDEST	23
h	0.200	Crime is TINV	5
i	0.182	Crime is TINFO	33
j	0.111	Crime is DATADEST	9
k	0.105	Crime is FRAUD	181
l	0.098	Victim is FIN	92
m	0.176	Victim is GOVT	51
n	0.064	Victim is COMPSERV	31
o	0.132	Victim is SALMFC	38

these computations is very small. The data points for entries g-k indicate that financial gain is the overwhelming motivation in most of these cases (181 points out of a total of 251).

Entries l-o indicate that, ceteris paribus, government computer security requirements appear to be less effective than those in the private sector. Among other things, this is probably attributable in part to differences in incentives in public versus private organizations.

Tables 25-48 display in matrix form the relationships between a number of variables deemed of interest.* We discuss only a select few of the tables as table content and interpretation are, for the most part, quite straightforward. These tables are based on the number of observations given in the

*Tables 25-48 are located together at the end of this section. The number of observations used in computing table entries varies from table to table. This arises from the fact that the data sets contain less than complete information on the variables of interest. Therefore, each table lists the maximum number of data points containing observations on each variable entering the table.

footnote under each table. No attempt was made to determine the statistical significance of individual entries in the tables or of the tables themselves. Nonetheless, most of the tables were calculated from quite a large number of incidents and hence deserve careful perusal.

Tables 25-28 contain distribution information on single variables. Table 26, for example, indicates that although almost two thirds of all cases involved a single adversary, eleven percent involved large conspiracies with five or more persons in collusion.

Tables 29 and 30 are concerned with the relationship between the type of crime (the objective of the perpetrator) and the position of the perpetrator. Table 29 indicates that, with the exception of students, the overwhelming objective of perpetrators is fraud, although theft of hardware and/or software was also an important goal for ex-employees. If we look at the other side of the picture and fix the crime category, we see in Table 30 that inventory thefts, information thefts, and fraud are dominated by executives and computer employees, with computer employees active in not only these areas but in all other crime categories as well.

Tables 32-36 show the relationship between loss size and a series of variables related to loss size. For example, Table 33 indicates that large losses are often associated with large conspiracies, as in Eq. (3) above. Table 35 shows that given a large loss is discovered, it most likely was the work of an executive with computer employees and outsiders running second. Again the regression equation bears out these observations. Tables 37-39 examine the relationship between the number of participants in an incident and the type or position of the participants. Table 38 points up another dimension of the threat posed by executives. Given that the number of perpetrators is large, say, 4 or more, executives are more likely to be involved in an incident than any other type of employee. The second most likely perpetrator is the generic noncomputer employee, a category which may also contain top management, since information in the sample on the position of perpetrators was often incomplete or very general as the case in noncomputer employee. It is not surprising that executives tend to be involved in conspiracies more often than other adversaries. The estimated loss equation indicates that collusion, on average, pays off; and since executives have more authority and moral suasion than other personnel within a firm, it should be easier for them to organize a conspiracy. It may also be true that since top executives rarely have day to day operating control over individual departments, they are forced to seek the participation of others.

Tables 40-43 examine the relationship between the type or category of crime, the location (insider-outsider), and number of perpetrators. Table 41 shows that inventory theft (Tinv) cases are usually undertaken by large groups; Table 42 shows that almost half of these cases involved both insiders and outsiders. But Table 43 shows that if an incident had been perpetrated by an outsider or by a combination of insiders and outsiders, then the odds are that the goal of the conspiracy was fraud.

Tables 44-46 contain information strictly in line with common sense perceptions of the type of threat various institutions face. Table 46 indicates that if fraud is uncovered, then the odds are that the victim is a financial institution, while unauthorized system use (Nuse) is most likely in educational institutions and computer service bureaus. If the crime discovered is theft of hardware or software (Thw/sw), data destruction (Datadest), or inventory theft (Tinv), the most likely victim is a firm in sales or manufacturing, while theft of information (Tinfo) is highest in government and in the computer service bureau industry. Each of these entries reinforces an earlier observation that relative opportunities play a large role in determining the type of system challenge chosen by an adversary. For example, there are certainly many fraud opportunities in government and in computer service bureaus, but these opportunities are overshadowed by the relative availability of proprietary information which is often highly marketable.

Tables 47 and 48 give information on the disposition of cases. Table 47 shows that if an incident is discovered and the perpetrator is known to be an executive, the probability of apprehension is 0.98, accompanied by about a 20% chance of being incarcerated. This is higher than for any other class of adversary. Table 48 indicates that if a case is discovered, there is a fairly high chance, 0.86, that the suspect will be apprehended; but given he is apprehended, the chance of going to prison is only one in nine. This finding reaffirms the widely held belief that sanctions for white-collar criminals are anything but severe. If a computer crime occurs, note that the probability that it will be discovered and the suspect(s) apprehended is only 0.13 (using the 15% standard estimate of discovery). Analogous calculations show that the estimated probability of incarceration (given discovery and apprehension) is only 0.014. These probabilities make computer crime an attractive proposition.

TABLE 25. Distribution of position (by highest ranking perpetrator): computer crimes, 1958-77.[a]

Perpetrator position	Probability
Executive	0.130
Computer employee	0.195
Noncomputer employee	0.149
Unknown employee	0.193
Corporation	0.035
Student	0.078
Ex-employee	0.030
Outsider	0.089
Unknown	0.101

[a] 461 sample points were available for these calculations.

TABLE 26. Distribution of number of perpetrators: computer crimes, 1958-77.[a]

Number of perpetrators	Probability
1	0.64
2	0.16
3	0.06
4	0.03
5 or more	0.11

[a] Total number of cases with data on each variable is 380. Rounding errors may cause totals to deviate from one.

TABLE 27. Distribution of type of crime: computer crimes, 1958-77.[a]

Crime category	Probability
Physical destruction	0.086
Theft of information	0.117
Theft of inventory	0.021
Data destruction	0.045
Theft of hardware or software	0.058
Unauthorized use	0.117
Fraud	0.538
Error[b]	0.018

[a] 461 incidents were available for these calculations.

[b] Error, of course, is not a crime category, but has been included for completeness. A few incidents which appear at first blush to involve criminal motivation, turn out upon further investigation, to be merely errors.

TABLE 28. Distribution of victim institution: computer crimes, 1958-77.[a]

Victim institution	Probability
Financial	0.320
Government	0.200
Medical	0.008
Educational	0.121
Sales/manufacturing	0.142
Communications and publishing	0.016
Transportation and utilities	0.031
Computer services	0.108
Profession organizations	0.013
Individual victim	0.041

[a] 388 sample points were available for these calculations.

TABLE 29. Distribution of crime category, conditional on perpetrator position: computer crimes, 1958-78.[a]

Given that perpetrator position[b] is:	Distribution of crime category[b] is:							
	Phydest	Tinfo	Tinv	Datadest	Thw/sw	Nuse	Fraud	Error[c]
Executive	0.016	0.150	0.050	0	0	0.066	0.716	0
Cemp	0.111	0.111	0.033	0.066	0.100	0.077	0.477	0.022
Ncemp	0	0.088	0.014	0.029	0.014	0.147	0.705	0
Unemp	0.034	0.113	0.022	0.090	0.045	0.090	0.602	0
Corp	0.062	0.187	0	0	0.125	0.125	0.312	0.187
Outsider	0.121	0.073	0	0.024	0.073	0.048	0.634	0.024
Student	0.250	0.166	0.055	0	0.027	0.388	0.083	0.027
Exemp	0	0.142	0	0.071	0.285	0.071	0.428	0
Unknown	0.244	0.111	0	0.022	0.066	0.133	0.422	0

[a] Total number of cases with data on each variable is 458. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

[c] Error, of course, is not a crime category, but has been included for completeness. A few incidents which at first blush appear to involve criminal motivation, turn out upon further investigation, to be merely errors.

TABLE 30. Distribution of perpetrator position, conditional on crime category: computer crimes, 1958-78.[a]

Given that crime	Distribution of perpetrator position[b] is:								
category[b] is:	Executive	Cemp	Ncemp	Unemp	Corp	Outsider	Student	Exemp	Unknown
Phydest	0.025	0.250	0	0.075	0.025	0.125	0.225	0	0.275
Tinfo	0.166	0.185	0.111	0.185	0.055	0.055	0.111	0.037	0.092
Tinv	0.272	0.276	0.090	0.181	0	0	0.181	0	0
Datadest	0	0.315	0.111	0.421	0	0.052	0	0.052	0.052
Thw/sw	0	0.333	0.037	0.148	0.074	0.111	0.037	0.148	0.111
Nuse	0.074	0.129	0.185	0.148	0.037	0.037	0.259	0.018	0.111
Fraud	0.174	0.174	0.195	0.215	0.026	0.105	0.012	0.024	0.077
Error	0	0.285	0	0	0.428	0.142	0.142	0	0

[a] Total number of cases with data on each variable is 458. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

TABLE 31. Distribution of loss size, conditional on perpetrator location: computer crimes, 1958-78.[a]

Given that perpetrator	Distribution of loss size ($1000) is:						
location is:	0-9	10-49	50-99	100-199	200-499	500-999	1000 and over
Insider(s)	0.31	0.22	0.08	0.14	0.07	0.03	0.14
Outsider(s)	0.32	0.06	0.16	0.16	0	0.13	0.16
Insider(s)/ outsider(s)	0.13	0.29	0.25	0.08	0.13	0.04	0.08

[a]Total number of cases with data on each variable is 232. Rounding errors may cause totals to deviate from one.

TABLE 32. Distribution of perpetrator(s) location, conditional on loss size: computer crimes, 1958-78.[a]

Given that loss size	Distribution of perpetrator location is:		
($1000) is:	Insider	Outsider	Insider/outsider
0-9	0.75	0.16	0.19
10-49	0.67	0.04	0.29
50-99	0.43	0.17	0.4
100-199	0.7	0.17	0.13
200-499	0.65	0	0.35
500-999	0.45	0.36	0.18
1000 and over	0.71	0.16	0.13

[a]Total number of cases with data on each variable is 232. Rounding errors may cause totals to deviate from one.

TABLE 33. Distribution of number of perpetrators, conditional on loss size: computer crimes, 1958-78.[a]

Given that loss size	Distribution of number of perpetrators is:				
($1000) is:	1	2	3	4	5 or more
0-9	0.74	0.13	0.07	0	0.07
10-49	0.64	0.19	0.04	0.04	0.09
50-99	0.52	0.16	0.06	0.1	0.16
100-199	0.67	0.15	0.04	0	0.15
200-499	0.56	0.06	0.06	0.13	0.19
500-999	0.44	0.22	0.11	0.11	0.11
1000 and over	0.44	0.12	0.04	0.12	0.28

[a] Total number of cases with data on each variable is 216. Rounding errors may cause totals to deviate from one.

TABLE 34. Distribution of loss size, conditional on number of perpetrators: computer crimes, 1958-78.[a]

Given that number of	Distribution of loss size ($1000) is:						
perpetrators is:	0-9	10-49	50-99	100-199	200-499	500-999	1000 and over
1	0.34	0.23	0.12	0.14	0.07	0.03	0.08
2	0.25	0.28	0.16	0.13	0.03	0.06	0.09
3	0.33	0.17	0.17	0.08	0.08	0.08	0.08
4	0	0.18	0.27	0	0.18	0.09	0.27
5 or more	0.14	0.14	0.18	0.14	0.11	0.04	0.25

[a] Total number of cases with data on each variable is 232. Rounding errors may cause totals to deviate from one.

TABLE 35. Distribution of perpetrator position, conditional on loss size: computer crimes, 1958-78.[a]

Given that loss size ($1000) is:	Distribution of perpetrator position[b] is:								
	Executive	Cemp	Ncemp	Unemp	Corp	Outsider	Student	Exemp	Unknown
0-9	0.13	0.2	0.19	0.17	0	0.09	0.07	0.01	0.14
10-49	0.14	0.18	0.25	0.24	0.04	0.04	0	0.08	0.04
50-99	0.16	0.26	0.16	0.23	0	0.16	0	0.03	0
100-199	0.3	0.07	0.13	0.2	0.03	0.17	0	0.07	0.03
200-499	0.29	0.18	0.12	0.18	0	0.06	0	0.06	0.12
500-999	0.25	0.08	0.17	0.17	0	0.25	0	0	0.08
1000 and over	0.22	0.22	0.03	0.16	0.09	0.16	0.06	0.03	0.03

[a] Total number of cases with data on each variable is 243. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

TABLE 36. Distribution of loss size, conditional on perpetrator position: computer crimes, 1958-78.[a]

Given that perpetrator	Distribution of loss size ($1000) is:						
position[b] is:	0-9	10-49	50-99	100-199	200-499	500-999	1000 and over
Executive	0.2	0.16	0.11	0.2	0.11	0.07	0.16
Cemp	0.32	0.20	0.18	0.05	0.07	0.02	0.16
Ncemp	0.33	0.32	0.13	0.1	0.05	0.05	0.03
Unemp	0.26	0.26	0.15	0.13	0.06	0.04	0.11
Corp	0	0.33	0	0.17	0	0	0.5
Outsider	0.22	0.07	0.19	0.19	0.04	0.11	0.19
Student	0.71	0	0	0	0	0	0.29[c]
Exemp	0.1	0.4	0.1	0.2	0.1	0	0.1
Unknown	0.59	0.12	0	0.06	0.12	0.06	0.06

[a] Total number of cases with data on each variable is 243. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

[c] There were only seven cases in which a student was the perpetrator, two of which involved very large losses.

TABLE 37. Joint distribution of number of perpetrators and perpetrator positions: computer crimes, 1958-78.[a]

Number of	Distribution of perpetrator position[b] is:								
perpetrators:	Executive	Cemp	Ncemp	Unemp	Corp	Outsider	Student	Exemp	Unknown
1	0.09	0.14	0.1	0.14	0	0.06	0.04	0.03	0.04
2	0.02	0.03	0.04	0.03	0	0.01	0.02	0.01	0
3	0.01	0.02	0.01	0	0	0.01	0.01	0	0
4	0.01	0.01	0.01	0	0	0	0	0	0
5 or more	0.02	0.01	0.02	0.03	0.01	0.01	0.01	0	0

[a] Total number of cases with data on each variable is 380. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

TABLE 38. Distribution of perpetrator position, conditional on number of perpetrators: computer crimes, 1958-78.[a]

Given that number of	Distribution of perpetrator position[b] is:								
perpetrators is:	Executive	Cemp	Ncemp	Unemp	Corp	Outsider	Student	Exemp	Unknown
1	0.15	0.22	0.16	0.21	0	0.09	0.07	0.05	0.06
2	0.15	0.22	0.25	0.17	0.02	0.07	0.1	0.03	0
3	0.18	0.32	0.14	0.05	0.05	0.09	0.18	0	0
4	0.38	0.23	0.23	0	0	0.08	0.08	0	0
5 or more	0.16	0.08	0.19	0.35	0.05	0.05	0.11	0	0

[a] Total number of cases with data on each variable is 380. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

TABLE 39. Distribution of number of perpetrators, conditional on perpetrator position: computer crimes, 1958-78.[a]

Given that perpetrator position[b] is:	Distribution of number of perpetrators is:				
	1	2	3	4	5 or more
Executive	0.6	0.15	0.07	0.08	0.1
Cemp	0.68	0.16	0.09	0.04	0.04
Ncemp	0.58	0.22	0.05	0.05	0.1
Unemp	0.69	0.13	0.01	0	0.17
Corp	0	0.25	0.25	0	0.5
Outsider	0.71	0.13	0.06	0.03	0.13
Student	0.53	0.19	0.13	0.03	0.13
Exemp	0.86	0.14	0	0	0
Unknown	1.0	0	0	0	0

[a] Total number of cases with data on each variable is 380. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

TABLE 40. Distribution of crime category, conditional on number of perpetrators: computer crimes, 1958-78.[a]

Given that number of perpetrators is:	Distribution of crime category[b] is:							
	Phydest	Tinfo	Tinv	Datadest	Thw/sw	Nuse	Fraud	Error[c]
1	0.07	0.1	0.01	0.07	0.07	0.11	0.56	0.01
2	0.03	0.16	0	0	0.03	0.18	0.59	0
3	0.09	0.09	0.04	0.04	0.04	0.22	0.43	0.04
4	0.14	0.14	0.21	0	0	0	0.5	0
5 or more	0.08	0.1	0.06	0.03	0.05	0.05	0.64	0

[a] Total number of cases with data on each variable is 381. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

[c] Error, of course, is not a crime category, but has been included for completeness. A few incidents which at first blush appear to involve criminal motivation, turn out upon further investigation, to be merely errors.

TABLE 41. Distribution of number of perpetrators, conditional on crime category: computer crimes, 1958-78.[a]

Given that crime category[b] is:	Distribution of number of perpetrators is:				
	1	2	3	4	5 or more
Phydest	0.65	0.08	0.08	0.08	0.12
Tinfo	0.58	0.23	0.05	0.05	0.09
Tinv	0.25	0	0.13	0.38	0.25
Datadest	0.89	0	0.05	0	0.05
Thw/sw	0.76	0.1	0.05	0	0.1
Nuse	0.61	0.24	0.11	0	0.04
Fraud	0.64	0.17	0.05	0.03	0.12
Error	0.75	0	0.25	0	0

[a] Total number of cases with data on each variable is 381. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

TABLE 42. Distribution of perpetrator location, conditional on crime category: computer crimes, 1958-78.[a]

Given that crime category[b] is:	Distribution of perpetrator location is:		
	Short	Medium	Long
Phydest	0.79	0.17	0.03
Tinfo	0.84	0.1	0.06
Tinv	0.56	0	0.44
Datadest	0.95	0.05	0
Thw/sw	0.83	0.17	0
Nuse	0.81	0.13	0.06
Fraud	0.66	0.12	0.22
Error	0.86	0.14	0

[a] Total number of cases with data on each variable is 136. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

TABLE 43. Distribution of crime category, conditional on perpetrator location: computer crimes, 1958-78.[a]

Given that	Distribution of crime category[b] is:							
perpetrator is:	Phydest	Tinfo	Tinv	Datadest	Thw/sw	Nuse	Fraud	Error
Insider	0.08	0.13	0.02	0.06	0.07	0.13	0.5	0.02
Outsider	0.1	0.1	0	0.02	0.08	0.12	0.56	0.02
Insider/ outsider	0.02	0.05	0.06	0	0	0.05	0.82	0

[a] Total number of cases with data on each variable is 416. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

TABLE 44. Distribution of perpetrator location, conditional on victim institution: computer crimes, 1958-78.[a]

Given that victim	Distribution of perpetrator location is:		
institution[b] is:	Insider	Outsider	Insider/outsider
Fin	0.61	0.19	0.21
Govt	0.67	0.1	0.23
Med	1.0	0	0
Educ	0.9	0.08	0.03
Salmfc	0.83	0.06	0.11
Compub	0.75	0.25	0
Transutil	0.67	0	0.33
Compserv	0.66	0.15	0.2
Proforg	0.6	0	0.4
Ind	0.88	0.06	0.06

[a] Total number of cases with data on each variable is 350. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

TABLE 45. Distribution of crime category, conditional on victim institution: computer crimes, 1958-78.[a]

Given that victim institution[b] is:	Distribution of crime category[b] is:							
	Phydest	Tinfo	Tinv	Datadest	Thw/sw	Nuse	Fraud	Error
Fin	0.04	0.01	0	0.02	0.01	0	0.93	0
Govt	0.03	0.18	0.04	0.03	0.03	0.11	0.58	0.01
Med	0.33	0	0	0	0	0	0.67	0
Educ	0.34	0.13	0	0.02	0.09	0.3	0.11	0.02
Salmfc	0.04	0.07	0.07	0.13	0.16	0.09	0.44	0
Compub	0	0.33	0	0	0.17	0	0.33	0.17
Tranutil	0.17	0	0.17	0	0	0	0.67	0
Compserv	0.05	0.26	0	0	0.14	0.24	0.31	0
Proforg	0.2	0.2	0	0.2	0	0	0.4	0
Ind	0	0.11	0	0	0	0.28	0.44	0.17

[a] Total number of cases with data on each variable is 388. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

TABLE 46. Distribution of victim institution, conditional on crime category: computer crimes, 1958-78.[a]

Given that crime	Distribution of victim institution[b] is:									
category[b] is:	Fin	Govt	Med	Educ	Salmfc	Compub	Tranutil	Compserv	Proforg	Ind
Phydest	0.161	0.064	0.032	0.516	0.064	0	0.064	0.064	0.032	0
Tinfo	0.024	0.341	0	0.146	0.097	0.048	0	0.268	0.024	0.048
Tinv	0	0.333	0	0	0.444	0	0.222	0	0	0
Datadest	0.153	0.153	0	0.076	0.538	0	0	0	0.076	0
Thw/sw	0.043	0.096	0	0.173	0.391	0.043	0	0.260	0	0
Nuse	0	0.190	0	0.333	0.119	0	0	0.238	0	0.119
Fraud	0.515	0.197	0.008	0.022	0.107	0.008	0.035	0.058	0.008	0.035
Error	0	0.166	0	0.166	0	0.166	0	0	0	0.500

[a] Total number of cases with data on each variable is 388. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

TABLE 47. Distribution of case disposition, conditional on perpetrator position: computer crimes, 1958-78.[a]

Given that	Distribution of disposition of case is:		
perpetrator position[b] is:	Suspect not apprehended	Suspect apprehended	Suspect incarcerated/apprehended
Executive	0.02	0.98	0.19
Cemp	0.13	0.88	0.11
Ncemp	0.07	0.93	0.15
Unemp	0.10	0.9	0.03
Outsider	0.18	0.82	0.14
Student	0.15	0.85	0.04
Exemp	0.08	0.92	0

[a] Total number of cases with data on each variable is 317. Rounding errors may cause totals to deviate from one.

[b] See Abbreviations and Definitions.

TABLE 48. Distribution of suspect dispositions: computer crimes, 1958-77.[a]

Disposition of suspect	Probability
Suspect not apprehended	0.138
Suspect apprehended	0.860
Suspect incarcerated[b]	0.099
Suspect incarcerated given suspect is apprehended[b]	0.115

[a] 312 incidents were available for these calculations.

[b] The probability a suspect is incarcerated is unconditional and represents the chance before apprehension that any given suspect will end up in prison. The last row presents the same probability after the suspect has been apprehended. Dividing the former by the latter obviously yields the chance of apprehension, 0.860.

DATA SET 3: EMPLOYEE DRUG THEFTS FROM DRUG MANUFACTURERS AND DISTRIBUTORS

The data on drug thefts were made available by the Drug Enforcement Administration (DEA). The data includes type and quantity of drug stolen by employees from drug manufacturers and distributors, street price of the drug, information on the number of drug audits and investigations performed by DEA, and information on the number and type of sanctions imposed for infractions of the regulatory code. Data on some of these variables were available by quarter from the third quarter of 1973 to the first quarter of 1978 for each of the thirteen DEA regulatory districts.* Other data series, e.g., street prices of drugs, were available for shorter periods. Information was also available on the quantities of various types of drugs reported by DEA as lost in transit. These data were collected because many DEA agents are convinced that a substantial portion of the drugs listed as lost in transit are actually stolen in transit--very often set up or fingered by employees of the manufacturer or distributor.

Drugs stolen by employees from drug manufacturers and distributors present quite a close analog to the insider theft problem potentially confronting NRC policy makers, especially for the case of the financially motivated adversary. In both the drug industry and the nuclear industry, a successful diversion involves removing physical quantities of material from a secured area--material that is monitored and accounted for throughout various stages of processing and which may well have deleterious effects on some subset of the population. In addition, both crimes depend upon a black market for material disposal.

This study assesses both the impact of street (or black market) prices of drugs and the impact of DEA imposed sanctions for violations of the regulatory code on the quantity of drugs stolen by insiders. The most serious weakness of the data set lies with the series on street prices of drugs. These series are compiled from street purchases of drugs made by DEA agents. The number of purchases at any point in time is usually quite small and the price variance from location to location can be high. The price data point for a given time period is the average of these purchases. Not enough purchases were

*See Appendix A for states and territories included in each region.

made to provide price information by region. Therefore, the price information we have available for each quarter may be viewed as a rough estimate of the national average price for the particular drug. The implication of this discussion for estimation is that the drug price series tends to contain considerable noise, but, hopefully not so much as to hide the role drug prices may play in explaining the quantity of drugs stolen by employees of drug manufacturers and distributors.

A second data weakness arises with the quantities stolen series. Experience in other areas and conversations with 1DEA agents indicate that a substantial portion of total drug thefts go undetected, whereas with the thefts that are detected, there exists powerful incentives on the part of managers to cover up shortages--in fact, the same incentives which may lead to MUF (material unaccounted for) coverups in the nuclear industry.* For each of these reasons the quantity stolen data series understates, and to some extent, masks the true relationship between the quantity stolen and the variables affecting the quantity stolen.

Prior to any data manipulation, we hypothesize that current and recent past street prices should be positively related to current period supply (quantity stolen) of any given drug. The higher the current and recent past, street price, the greater the incentive for suppliers to steal now and enjoy the high return.

Economic theory states that any relationship purporting to explain quantities being offered for sale (either in legal or illegal markets) must include measures of the return (price) in substitute income generating alternatives, both legal and illegal. In the case at hand, the unit return (price) from substitute legal and illegal activities should appear in illicit drug supply equations with negative coefficients indicating that the activities are alternative sources of income. For example, an equation explaining amphetamine thefts should include a measure of legal earning possibilities as well as the price of, say barbiturates, a measure of returns in alternative

*Since the regulatory code in each industry frowns upon shortages, managers may find it in their interest not to report missing material. Also reporting missing material results in a distinct possibility that the shortage will become public information (via freedom of information (FOI) suits, e.g.) with the concomitant undesirable publicity.

drug related illegal endeavors. But if regional per capita income is used to proxy for returns in legal income generating activities, the theory leaves ambiguous the nature of the relation between per capita legal income in a region and drug supplies in the region. The precise nature of this relation is ambiguous because the higher the legal income in an area, the fewer the number of individuals willing to enter the risky occupation of stealing drugs. In other words, regional per capita income is a measure, on average, of alternative legal income sources--the higher the alternative income generating prospects, *ceteris paribus*, the lower the supply of effort devoted to the risky illegal activity. On the demand side of the illegal drug market the higher the income level in a region, the greater the purchasing power, *ceteris paribus*, the more drugs suppliers will be able to sell at any given price. In summary, on the supply side of the illegal drug market, the income variable measures alternative (legal) income producing sources for suppliers or potential suppliers and is negatively related to drug supplies. On the demand side of the illegal drug market, the income variable measures purchasing power in the region and, *ceteris paribus*, should be positively related to the quantity of drugs sold in a region. Since income enters both demand and supply equations with opposite signs is is not possible, *a priori*, to know the sign of the income coefficient in an estimated equation.

As far as measures of the sanctions DEA may impose for violations of regulatory code are concerned, we have used average values of these variables over the two most recent quarters to measure their effects. More specifically, five different categories of sanctions are used by DEA to bring errant manufacturers and distributors into line with the regulatory code. In order of increasing severity, firms may receive: (1) a warning from a DEA agent to improve certain procedures and/or not to permit a given violation to reoccur; (2) the firm may receive a letter of admonition if a warning is not deemed sufficient; (3) DEA may require attendance at an administrative hearing if, e.g., an infraction that merited a warning or letter of admonition was not rectified or if the original infraction was later determined to be more serious; (4) DEA may seize drugs from the firm if appropriate efforts are not made to straighten out code violations or if infractions are severe; and, (5) DEA may arrest involved parties in cases of suspected criminal noncompliance with the code.

Conversations with DEA agents indicated that agent warnings, letters of admonition, and even administrative hearings are viewed as mere slaps on the wrist by manufacturers and distributors and essentially mean that the case is closed without any meaningful penalty. If this is indeed the case, we might expect to find the level of these variables to be positively related to illicit drug supplies, since increases in the levels of these perfunctory measures, ceteris paribus, imply a decrease in the overall severity of sanctions.[*] Equation (4) uses the number of administrative hearings in a region to represent the class of perfunctory enforcement measures, although we have experimented with each of the other variables. To represent the class of strong enforcement measures, we have used only the number of arrests made by DEA in a region, since there were not enough instances of drug seizures in the sample to permit use of this variable.

Data were available on thefts of amphetamines, barbiturates, cocaine and narcotics by employees of the manufacturers and distributors of these drugs[†] and on the quantity of these same drugs listed by DEA as lost in transit. Since in all cases the estimation results for each drug are more or less similar, we report only one estimated equation which attempts to explain insider thefts and one estimated equation which attempts to explain the quantity of drugs lost in transit. The former estimate is reported next.

$$\begin{aligned} AMPIN_t = {} & \underset{(10.1098)}{7.3428} + \underset{(0.0578)}{0.0909}\, PAMP_t + \underset{(0.0008)}{0.0009}\, TAMPIN_{t-1} - \underset{(0.0329)}{0.0718}\, PBARB_{t-1} \\ & - \underset{(1.1090)}{0.4116} Y_t + \underset{(0.5243)}{0.8971}\, AHEAR - \underset{(2.0455)}{3.4148}\, ARREST \end{aligned} \tag{4}$$

$$F(6,\ 90) = 1.77,\ (P_r > F) = 0.115,$$

[*] Note: The five sanctions are not, in theory, mutually exclusive, but in practice tend to be. For example, an administrative hearing presumably could lead to findings that result in an arrest. But this does not appear to be the case. Such hearings seem to be used by DEA to warn firms against further infractions and not for fact finding.

[†] Narcotics include morphine, codeine, heroin, methadone, etc. Barbiturates are members of a broad class of drugs generically called depressants. Cocaine and amphetamines are both stimulants. Cocaine is often mistakenly classified as a narcotic, but unlike narcotics, cocaine is either not habit forming or at worst, only mildly so.

where

$AMPIN_t$ = dosage units of amphetamines stolen by insiders in a region in quarter t divided by the number of manufacturers and distributors in that region,*

$PAMP_t$ = price (street) of amphetamines in quarter t, in dollars per 1000 dosage units,

$PBARB_t$ = price (street) of barbiturates in quarter t in dollars per 1000 dosage units,

Y_t = regional per capita income in quarter t,†

AHEAR = the average number of administrative hearings in a region in quarters t - 1 and t - 2,**

ARREST = the average number of arrests for drug code violations in a region in quarter t - 1 and t - 2,** and

$TAMPIN_t$ = total dosage units of amphetamines stolen by insiders in a region in quarter t.

Recall that street drug price data were available only on a nationwide basis and not on a regional basis and that we have used an average of past sanction levels to explain present drug supplies. The hypothesis here is that suppliers and potential suppliers of illegal drugs use past penalty levels to draw conclusions about present penalties if they are caught. As has been the case throughout the report, the number in parenthesis under each estimated coefficient is the standard error and the symbol $F(\alpha, \beta)$ is the estimated F statistic with α degrees of freedom in the numerator and β degrees of freedom in the denominator.

*We used the number of drug manufacturers and distributors in a region as a proxy for the size of the drug industry in the region and thus standardized dosage units stolen by employees in a region by the size of the industry in the region.

†Regional refers to DEA regions. Regional per capita incomes were calculated using a population weighted average of state per capita incomes.

**Past sanction levels alone are used in the estimated equation. The hypothesis that leads to this specification is that potential suppliers project current sanction levels by looking at the recent past. In addition, suppliers most likely will not know "current" sanction levels until after the current period is over. Notice that this will not be the case for prices. Potential suppliers can obtain current black market prices merely by asking the person or persons to whom they usually sell the stolen drugs for a current quotation. Hence current, and perhaps lagged, prices but only lagged sanctions enter the supply equation.

Given the quality of the data, and in particular the street price data, our equation explains the relative quantities of amphetamines stolen by employees reasonably well. First, current street prices of amphetamines are positively related to current quantities of amphetamines stolen.* The coefficient of lagged barbiturate prices cause supplies of stolen amphetamines to decrease as suppliers presumably begin stealing more barbiturates and fewer amphetamines. In the eyes of perpetrators amphetamine and barbiturate thefts are alternative means of generating income--which is stolen depends upon relative profitability. Current prices of barbiturates and past prices of amphetamines also were entered into estimated equations and were found to be totally ineffective in explaining current quantities of amphetamines stolen. Apparently amphetamine suppliers are affected most by current selling prices of amphetamines and use past prices of substitutes as an indicator of present demand conditions. Of course, we would expect suppliers of drug X to have prices of X immediately available, while current prices of substitutes may not be as easy to come by. If this is the case, past prices of substitutes may be used as a proxy for current prices, as our equation suggests. In Eq. (4) the coefficient of per capita income is negative but insignificant, indicating that the demand side and supply side effects of (legal) income on drug thefts are of the same approximate magnitude and hence tend to cancel out. Next note that the two sanction variables have significant coefficients of the sign we expected in our discussion above. Apparently it is true that perfunctory slap on the wrist type sanctions, such as administrative hearings, can actually provide an incentive to perpetrators of drug thefts.† As we have argued, an increase in such sanctions, all else being the same, implies a reduction in the overall severity of penalties and hence will have an incentive effect on the suppliers of stolen drugs. Increases in the number of arrests, however, causes a reduction in quantities of drugs stolen. Finally, we have included total amphetamine losses to insiders in the past quarter in the estimated equation. To the extent that a drug is habit forming, past thefts (and sales)

*The coefficient of $PAMP_t$ is significant only at the 0.10 level. We also experimented with lagged prices of amphetamines, but found them to be statistically insignificant at any meaningful level.

†We estimated equations using each of the perfunctory sanctions. The agent warning variable and the letter of admonition each entered estimated equations with positive coefficients, but were not as strong as the administrative hearing variable. Entering more than one of these variables in an equation decreases the significance of the equation.

should be positively related to present thefts (and sales). The coefficient is positive but not very precise. With strong habit forming drugs this coefficient should be much more precise (see Eq. (5) below).

Several inferences drawn from Eq. (4) may well be transferable to the nuclear industry. The primary points are that high black market prices provide incentives to insiders to engage in risky illegal activities. Hence existence of established black markets for SNM (special nuclear materials) with high prices should be viewed as a warning to those responsible for the safety of these materials. In general, our analysis indicates that the higher the price, the greater the threat, since more and more individuals will be tempted as the price rises and existing thieves will be tempted to steal more. Second, care should be taken in the design of sanctions. The estimated equation indicates that increases in the use of mild sanctions relative to more severe measures for infractions, actually have incentive effects on suppliers and potential suppliers of the illegal activity. Finally, policy makers should ignore arguments to the effect that increased enforcement has little influence on behavior. In Eq. (4) above--using the number of arrests as our measure of enforcement credibility--and in all other internal security threat studies with which we are familiar, reasonable measures of enforcement and penalty severity turn out to be negatively related to associated illegal activity levels.

The F statistic reported after Eq. (4) indicates that the estimated equation is significant at the 0.115 level.* Intuitively, this means that the set of independent variables included in Eq. (4), as a group have a nonzero affect on insider amphetamine thefts with probability 0.89. Hence we are reasonably sure that prices, and enforcement levels are important factors in determining the supply of stolen amphetamines.

We now report the results of a regression analysis using total dosage units of narcotics lost in transit in a region, relative to the total number of drug manufacturers and distributors in the region, as the dependent

*Here as in each estimated equation, we are implicitly either making certain assumptions about the distribution of equation disturbances or calling on the central limit theorem to permit calculation of these significance levels. See any mathematical statistics or econometrics text for more detail.

variable.* Equations were estimated for each of the drug categories mentioned above. The narcotics equation seemed to be the least volatile to small changes in the sample so we elected to report it. But, again, each of the estimated equations displayed similar qualitative properties.

$$\mathrm{NARCLIT}_t = \underset{(103.79)}{-\ 80.47} + \underset{(29.22)}{24.40}\ \mathrm{PHER}_{t-1} - \underset{(126.97)}{182.99}\ \mathrm{PCOC}_{t-1} + \underset{(15.40)}{26.25}\ Y_t \qquad (5)$$

$$+ \underset{(7.86)}{24.81}\ \mathrm{AHEAR} - \underset{(31.67)}{67.97}\ \mathrm{ARREST} + \underset{(0.0003)}{0.0009}\ \mathrm{TNARCLIT}_{t-1}$$

$$F(6,103) = 5.03 \quad (\Pr > F) = 0.0002,$$

where

$\mathrm{NARCLIT}_t$ = total number of dosage units of narcotics reported as lost in transit from manufacturers and distributors in a DEA region in quarter t divided by the number of manufacturers and distributors in that region,

PHER_t = the street price of heroin in quarter t in dollars per milligram of 100% pure heroin (since heroin is a narcotic and no price index for narcotics was available, we have [illegible]oin prices as a proxy for all narcotic prices)

PCOC_t = the street price of cocaine in quarter t in dollars per milligram of 100% pure cocaine, and

$\mathrm{TNARCLIT}_t$ = total number of dosage units of narcotics lost in transit in quarter t in a DEA region.

Equation (5) shows that the price of heroin in the past quarter is positively related to the number of dosage units of narcotics lost in transit. Although the estimated coefficient is not very precise, it does arouse suspicion when quantity of drug lost in transit increases with the street price of the same drug.

*We used the number of drug manufacturers and distributors in a region as a proxy for the size of the drug industry in the region and thus standardized dosage units lost in transit in a region by the size of the industry in the region.

Adding to suspicion as to the nature of transit losses, is the fact that the unit return to a substitute illegal source of income, the price of cocaine, turns out to be negatively related to the amount of narcotics lost in transit. The higher the street price of cocaine (the unit return to stealing cocaine), the fewer narcotics lost in transit. Although again this estimate is imprecise, the narcotics lost in transit variable behaves in a manner consistent with the hypothesis that a substantial portion of all narcotics lost in transit are not actually lost at all, but are stolen. This impression is reinforced by the coefficients of the two enforcement variables AHEAR and ARREST which have the same sign as in the insider theft equation above--and these coefficients are significantly different from zero under usual conventions. Finally, we have added the total amount of narcotics stolen in the previous quarter to our independent variables, which also turns out to be statistically significant.* Our hypothesis here is that since narcotics are habit-forming, last quarter's sales should contain information about present sales levels and therefore drug supply information. As reported, the estimated equation has an associated F statistic with a value of 5.03, which makes the estimated equation significant at the 0.0002 level. Roughly, we are sure with probability 0.9998 that the included set of independent variables have a nonzero impact in explaining narcotics lost in transit. Of course, some portion of those drugs reported as lost in transit may actually be lost in transit. Our analysis suggests that a significant portion of the total is not lost, but stolen.

*Recall that the lagged value of amphetamines stolen by insiders was entered into the insider theft equation above, but was insignificant. We argued there that the more addictive the drug, the more information lagged values of thefts (and hence sales) will contain about current thefts (and sales). This argument receives support from the coefficient of TNARCLIT_{t-1} in Eq. (5).

SUMMARY

In conclusion, we would like to re-emphasize the closeness of the analog between insider thefts of drugs from manufacturers and distributors and insider thefts of SNM from reprocessing plants or reactors, especially for financially motivated adversaries. In each case, the industry is under strict federal regulation. Special inventory and accounting methods are used to control plant inventories and throughput. A successful diversion requires removal of physical quantities of material from a secured area, and removal and distribution or sale of the stolen material by the adversary is likely to have serious debilitating consequences for some subset of the population. In addition, a black market is needed to dispose of stolen materials in each case.

Our analysis of the drug data supports a number of conclusions which should be of interest to those concerned with security in the nuclear industry: (1) insider thefts of a given drug are positively related to current prices of the drug--the higher the price, the higher the predicted quantities stolen. So by analogy, periods of high and rising SNM (black market) prices should be viewed as periods when special vigilance is required; (2) since prices of substitute income generating activities enter the estimated "insider" drug supply equation, we conclude that drug thieves and potential drug thieves view their activities in much the same way as those engaged exclusively in legal activities. They respond to differential rates of return and allocate their time to endeavors in which expected returns are highest. This has especially ominous implications vis-a-vis organized crime, if black market prices of SNM rise enough to overshadow returns from drugs, prostitution, and other mainstays of organized crime; (3) if the federal regulatory code designates a series of sanctions for code infractions, policy makers must be aware that increasing the use of perfunctory sanctions may, ceteris paribus, actually lead to increases in the activity the sanction was designed to curtail. This point was brought out in both the estimated equations by the positive coefficient on the administrative hearing variable; (4) each of the equations reported implies that increasing enforcement, as measured by the number of arrests, will have unambiguous deterrent effects on drug suppliers; (5) our analysis of the lost in transit data tended to support the suspicions of the DEA agents we spoke to--viz., that a good portion of all drugs lost in transit are actually stolen. (The same variables that explain insider thefts also do a reasonable job in explaining drugs lost in transit.)

In addition, since the number of incidents in which drugs are lost in transit are thirty-three times larger than the number of cases in which insiders are involved in a drug theft, we may conclude that transportation represents a weak link in the drug control and accounting system. Drugs being transported are apparently relatively easy to access via an inside adversary. The analog for SNM is obvious. Table 49 lists the source of drug theft losses. Note that although only 2% of all cases of drug thefts involve insiders, insiders represent almost 20% of total losses.

TABLE 49. Relative importance of drug losses from manufacturers and distributors by type of incident, 1973-77.[a]

	Type of incident					
Units of measurement	Night break in	Armed robbery	Employee pilferage	Customer theft	Lost in transit	Other thefts
Number of incidents ÷ total of incidents	0.023	0.006	0.020	0.021	0.657	0.264
Dosage units stolen ÷ total dosage units stolen	0.062	0.015	0.195	0.012	0.542	0.171

[a] Total number of cases with data on both variables is 247.

APPENDIX

DEA REGIONS

DEA Region	States or Territories
Region 1	CT, MA, ME, NH, RI, VT
Region 2	NY
Region 3	DE, PA
Region 4	DC, MD, NC, VA, WV
Region 5	Misc. Carib. Is., FL, GA, PR, SC, Swan Islands, Virgin Islands
Region 6	KY, MI, OH
Region 7	IL, IN, WI
Region 8	AL, AR, LA, MS, TN
Region 9	(Does not exist)
Region 10	IA, KS, MN, MO, NB, ND, SD
Region 11	OK, TX
Region 12	AZ, CO, NM, UT, WY
Region 13	AK, ID, MT, OR, WA
Region 14	CA, HI, NV

U.S. GOVERNMENT PRINTING OFFICE 1980 -0- 620-269/253

NRC FORM 335
(7-77)

U.S. NUCLEAR REGULATORY COMMISSION

BIBLIOGRAPHIC DATA SHEET

1. REPORT NUMBER (Assigned by DDC)
NUREG/CR-1234
UCRL-52744

4. TITLE AND SUBTITLE (Add Volume No., if appropriate)
The Insider Threat to Secure Facilities: Data Analysis

2. (Leave blank)

3. RECIPIENT'S ACCESSION NO

7. AUTHOR(S)
J. M. Heineke and Associates

5. DATE REPORT COMPLETED
MONTH May | YEAR 1980

9. PERFORMING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Lawrence Livermore National Laboratory
NSS Safeguards Program, L-97
P. O. Box 808
Livermore, CA 94550

DATE REPORT ISSUED
MONTH June | YEAR 1980

6. (Leave blank)

8. (Leave blank)

12. SPONSORING ORGANIZATION NAME AND MAILING ADDRESS (Include Zip Code)
Division of Safeguards, Fuel Cycle & Environmental Research
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

10. PROJECT/TASK/WORK UNIT NO.

11. CONTRACT NO.
FIN No. A0132

13. TYPE OF REPORT
NUREG

PERIOD COVERED (Inclusive dates)

15. SUPPLEMENTARY NOTES

14. (Leave blank)

16. ABSTRACT (200 words or less)

Three data sets drawn from industries that have experienced internal security breaches are analyzed. The industries and the insider security breaches are considered analogous in one or more respects to insider threats potentially confronting managers in the nuclear industry. The three data sets are: bank fraud and embezzlement (BF&E), computer-related crime, and drug theft from drug manufacturers and distributors. A careful analysis by both descriptive and formal statistical techniques permits certain general conclusions on the internal threat to secure industries to be drawn. These conclusions are discussed and related to the potential insider threat in the nuclear industry.

17. KEY WORDS AND DOCUMENT ANALYSIS

17a. DESCRIPTORS

17b. IDENTIFIERS/OPEN-ENDED TERMS

18. AVAILABILITY STATEMENT
Unlimited

19. SECURITY CLASS (This report)
Unclassified

21. NO. OF PAGES
72

20. SECURITY CLASS (This page)
Unclassified

22. PRICE
S

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

OFFICIAL BUSINESS
PENALTY FOR PRIVATE USE, $300

POSTAGE AND FEES PAID
U.S. NUCLEAR REGULATORY
COMMISSION

U.S. MAIL

DOCUMENT CONTROL DESK
016
555

NUREG/CR-1234 THE INSIDER THREAT TO SECURE FACILITIES: DATA ANALYSIS JUNE 1980