POTENTIAL THREAT TO LICENSED NUCLEAR ACTIVITIES FROM INSIDERS

(INSIDER STUDY)

Sarah A. Mullen
John J. Davidson
Harvey B. Jones, Jr.

May 9, 1980

Physical Security Development Branch
Division of Safeguards
Office of Nuclear Material Safety and Safeguards

CONTENTS

	PAGE
LIST OF FIGURES.	iv
LIST OF TABLES	vi
ACKNOWLEDGMENTS.	ix
1. EXECUTIVE SUMMARY	1
2. INTRODUCTION.	2-1
2.1 Objective.	2-1
2.2 Background	2-1
2.2.1 Transition from Generic Adversary Characteristics Study.	2-2
2.2.2 Current Threat Definitions.	2-2
2.2.2.1 Protection against Theft or Diversion of Formula Quantities of Strategic Special Nuclear Material (SSNM)	2-3
2.2.2.2 Protection against Radiological Sabotage . .	2-3
2.2.3 Other Considerations	2-4
2.2.3.1 General Impact of White-Collar Theft	2-4
2.2.3.2 Proposed Clearance Rule.	2-5
2.2.3.3 Lawrence Livermore Laboratory Research . . .	2-6
2.3 Scope.	2-7
2.3.1 General	2-7
2.3.2 Adversary Characteristics	2-8
2.3.3 Security System Vulnerabilities	2-8
2.3.4 Detection/Prevention Strategies	2-8
2.4 Limitations.	2-9
2.4.1 Scope	2-9
2.4.2 Data.	2-10
2.5 Sources.	2-11
2.5.1 Analog Data	2-11
2.5.2 Nuclear Data.	2-11
2.5.3 Open-Source Data.	2-11

CONTENTS (Continued)

		PAGE
2.6	Approach.	2-12
2.6.1	Use of Analogs	2-12
2.6.2	Case Histories--Objective Data	2-13
2.6.2.1	Analog Development.	2-13
2.6.2.2	Adversary Characteristics	2-15
2.6.2.3	Security System Vulnerabilities	2-17
2.6.2.4	Detection/Prevention Strategies	2-17
2.6.3	Expert Opinion--Subjective Data.	2-17
3.	ANALYSIS OF THE INSIDER ADVERSARY.	3-1
3.1	Implications for Nuclear Safeguards	3-1
3.1.1	General.	3-1
3.1.2	Insider Behavior in a Strong Safeguards Environment. .	3-1
3.1.3	Saboteur vs. Thief	3-2
3.1.4	Theft Conspiracies vs. Single Insider Thefts	3-3
3.2	Insider Thief	3-3
3.2.1	Behavior Patterns.	3-3
3.2.1.1	Target Control.	3-3
3.2.1.2	Group Size.	3-6
3.2.2	Characteristics Profile.	3-7
3.3	Insider Saboteur--Characteristics Profile	3-12
4.	SECURITY SYSTEM VULNERABILITIES TO THE INSIDER	4-1
4.1	Introduction.	4-1
4.2	Implications for Nuclear Safeguards	4-1
4.3	Analysis of Insider Cases and Expert Opinion.	4-2
4.3.1	Inconsistent Application of Security Procedures . . .	4-2
4.3.2	Failure to Separate and Rotate Duties.	4-3
4.3.3	Excessive Trust Due to Longevity or Position	4-4
4.3.4	Personnel Security Deficiencies.	4-5
4.3.5	System Design Deficiencies	4-6

CONTENTS (Continued)

	PAGE
5. DETECTION AND PREVENTION STRATEGIES.	5-1
5.1 Introduction.	5-1
5.2 Implications for Nuclear Safeguards	5-1
5.2.1 Detection.	5-1
5.2.2 Prevention	5-3
5.3 Analysis of Detection Strategies.	5-4
5.3.1 Insider Cases.	5-4
5.3.2 Non-NRC Studies and Expert Opinion	5-9
5.4 Analysis of Prevention Strategies	5-14
5.4.1 Insider Cases.	5-14
5.4.2 Non-NRC Studies and Expert Opinion	5-15
5.4.2.1 Preemployment Screening and Clearances. . . .	5-16
5.4.2.2 Behavioral Observation Programs	5-23
5.4.2.3 Psychological Assessment Techniques	5-28
5.4.2.4 Management-Employee, Management-Security and Security-Employee Rapport.	5-30
5.4.2.5 Other Prevention Strategies	5-33
APPENDIX A - LIST OF ACKNOWLEDGMENTS.	A-1
APPENDIX B - LAWRENCE LIVERMORE LABORATORY RESEARCH	B-1
APPENDIX C - NUCLEAR EVENTS	C-1
APPENDIX D - GLOSSARY OF TERMS.	D-1
APPENDIX E - ANALOGOUS INDUSTRIES	E-1
APPENDIX F - SPECIAL CASES.	F-1
APPENDIX G - FIGURES AND TABLES	G-1
APPENDIX H - BIBLIOGRAPHY	H-1

LIST OF FIGURES

NUMBER	TITLE	PAGE
G.1	Distribution of Types of Target Control: Theft, Analogs 1 & 2	G-1
G.2	Distribution of Types of Target Control: Theft, Analog 1 & 2 Comparison.	G-2
G.3	Distribution of Levels of Screening: Theft, Analogs 1 & 2 .	G-3
G.4	Distribution of Types of Access: Theft, Analogs 1 & 2 . . .	G-4
G.5	Distribution of Types of Access: Theft, Analog 1 & 2 Comparison.	G-5
G.6	Distribution of Length of Service: Theft, Analog 1 & 2 Comparison.	G-6
G.7	Distribution of Levels of Training: Theft, Analog 1 & 2 Comparison.	G-7
G.8	Distribution of Types of Stimuli: Theft Analog 1 & 2 Comparison.	G-8
G.9	Distribution of Levels of Dedication: Theft, Analog 1 & 2 Comparison.	G-9
G.10	Distribution of Insider Group Size: Theft, Analogs 1 & 2. .	G-10
G.11	Distribution of Insider Group Size: Theft Analog 1 & 2 Comparison.	G-11
G.12	Distribution of Outsider Involvement: Theft, Analog 1 & 2 Comparison.	G-12
G.13	Distribution of Types of Role: Theft, Analogs 1 & 2	G-13
G.14	Distribution of Types of Role: Theft, Analog 1 & 2 Comparison.	G-14
G.15	Distribution of Levels of Planning: Theft, Analog 1 & 2 Comparison.	G-15
G.16	Distribution of Types of Target Control: Sabotage	G-16

LIST OF FIGURES (Continued)

NUMBER	TITLE	PAGE
G.17	Distribution of Levels of Screening: Sabotage	G-17
G.18	Distribution of Types of Access: Sabotage	G-18
G.19	Distribution of Lengths of Service: Sabotage.	G-19
G.20	Distribution of Levels of Training and Skills: Sabotage . .	G-20
G.21	Distribution of Types of Motivations: Sabotage.	G-21
G.22	Distribution of Levels of Dedication: Sabotage.	G-22
G.23	Distribution of Insider Group Size: Sabotage.	G-23
G.24	Distribution of Types of Role: Sabotage	G-24
G.25	Distribution of Levels of Planning: Sabotage.	G-25
G.26	Comparison of Distribution of Methods of Detection: Theft (Analog 1 and 2) and Sabotage (Analog 1 and 2 and Special Cases).	G-26

LIST OF TABLES (Continued)

NUMBER	TITLE	PAGE
B.1	Predicted Losses, Perpetrator Position and Bank Size.	B-3
B.2	Distribution of Collusive Attacks on Banks, Conditional On Perpetrator Position: BF&E Cases, 1976-77.	B-5
B.3	Distribution of Conspiracy Size, Conditional on Position of Perpetrator: BF&E Cases, 1976-77	B-5
B.4	Distribution of Group Size: BF&E Cases, 1976-77.	B-5
B.5	Distribution of Perpetrators by Type of Group: BF&E Cases, 1976-77.	B-6
B.6	Predicted Losses, the Number of Perpetrators and Bank Size. .	B-6
B.7	Predicted Losses, Employee Bond Coverage and Bank Size. . . .	B-7
B.8	Distribution of Method of Detection, Conditional on Position of Perpetrator: BF&E Cases, 1976-77	B-9
B.9	Distribution of Method of Detection, Conditional on Number of Perpetrators: BF&E Cases, 1976-77.	B-10
B.10	Frequency of Detection by Method: BF&E Cases, 1976-77. . . .	B-10
B.11	Distribution of Time Concealed, Conditional on Perpetrator Position: BF&E Cases, 1976-77	B-11
B.12	Predicted Losses and the Number and Type of Perpetrator: Computer crimes.	B-17
B.13	Distribution of Perpetrator Position, Conditional on Number of Perpetrators: Computer Crimes, 1958-78.	B-18
B.14	Predicted Losses, Outsider Involvement, Number and Type of Perpetrator: Computer Crimes.	B-19
B.15	Distribution of Number of Perpetrators: Computer Crimes, 1958-77.	B-20
B.16	Distribution of Type of Crime: Computer Crimes, 1958-77. . .	B-21
B.17	Distribution of Number of Perpetrators, Conditional on Crime Category: Computer Crimes, 1958-78.	B-22
B.18	Distribution of Perpetrator Location Conditional on Crime Category: Computer Crimes 1958-78	B-22

LIST OF TABLES (Continued)

NUMBER	TITLE	PAGE
B.19	Predicted Losses, Victim Institution and Type of Perpetrator: Computer Crimes.	B-23
B.20	Distribution of Crime Category, Conditional on Victimized Institution: Computer Crimes, 1958-78	B-24
B.21	Distribution of Perpetrator Location, Conditional on Victimized Institution: Computer Crimes, 1958-78.	B-25
B.22	Estimated Probabilities of Success: Computer Crimes.	B-26
B.23	Drug Losses from Manufacturers and Distributors by Type of Incident--Relative Importance, 1973-77	B-30
G.1	Distribution of Most Frequent Motivations by Target Control Type: Theft: Analogs 1 & 2	G-27
G.2	Distribution of Types of Access by Target Control Type: Theft, Analogs 1 & 2.	G-28
G.3	Distribution of Types of Role by Target Control Type: Theft, Analogs 1 & 2.	G-28
G.4	Distribution of Types of Stimuli by Target Control Type: Theft, Analogs 1 & 2.	G-29
G.5	Distribution of Levels of Planning by Target Control Type: Theft, Analogs 1 & 2.	G-30
G.6	Distribution of Degrees of Outside Involvement by Target Control Type: Theft, Analogs 1 & 2	G-30
G.7	Distribution of Tactics by Target Control Type: Theft, Analogs 1 & 2	G-31
G.8	Distribution of Tactics Involving Manipulation of Procedures and Resources by Target Control Type: Theft, Analogs 1 & 2	G-32
G.9	Distribution of Tactics Involving Subterfuge by Target Control Type: Theft, Analogs 1 & 2	G-32
G.10	Distribution of Motivations: Theft, Analog 1 and 2 Comparison.	G-33
G.11	Complete Distribution of Motivations: Theft, Analog 1 and 2 Comparison	G-34
G.12	Distribution of Tactics: Theft, Analog 1 & 2 Comparison . .	G-35
G.13	Complete Distribution of Tactics: Theft, Analog 1 and 2 Comparison	G-36

LIST OF TABLES

NUMBER	TITLE	PAGE
G.14	Complete Distribution of Motivations: Sabotage (Analog 1, 2 and Special Cases)	G-37
G.15	Complete Distribution of Tactics: Sabotage (Analog 1, 2 and Special Cases)	G-38
G.16	Distribution of Method of Detection: Theft, Analog 1. . . .	G-39
G.17	Distribution of Method of Detection: Theft, Analog 2. . . .	G-39
G.18	Distribution of Method of Detection Conditional upon Target Control of Insiders: Theft (Analog 1 and 2) vs. Sabotage (Analog 1 and 2 and Special Cases)	G-40
G.19	Distribution of Method of Detection Conditional upon Role of Insider: Theft, Analog 1 and 2.	G-41
G.20	Distribution of Method of Detection Conditional upon Number of Insiders: Theft (Analog 1 and 2) vs. Sabotage (Analog 1 and 2, Special Cases)	G-42
G.21	Distribution of Method of Detection Conditional upon Insider/Outsider Conspriracy: Theft, Analog 1 & 2.	G-43
G.22	Distribution of Insider Group Size Conditional upon Level of Screening: Theft, Analog 1 and 2	G-44
G.23	Distribution of Insider Group Size Conditional upon Level of Screening: Sabotage, Analog 1 and 2 and Special Cases. .	G-44
G.24	Distribution of Length of Service Conditional upon Level of Screening: Theft, Analog 1 and 2	G-45
G.25	Comparison of PRP Disqualification Causes	G-46

ACKNOWLEDGMENTS

The study group wishes to acknowledge the valuable advice and technical guidance provided to it by the study's Coordinating Committee, comprised of senior staff members from the Division of Safeguards, and by the inter-office Steering Committee, comprised of representatives from the NRC Offices of Nuclear Reactor Regulation, Inspection and Enforcement, and Standards Development. Special thanks go to two members of the Division of Safeguards' Physical Security Development Branch: Mr. Charles South, for his much-appreciated assistance in the organizational and conceptual phases of the project, and Dr. John Hockert for his unselfish analytical support. Mr. Joseph Yardumian of the Technical Planning and Information Branch, Division of Safeguards, was instrumental in the study's start-up phase.

Special mention must be made of three dedicated consultants whose interviews with security experts in analogous industries across the nation provided a significant portion of the study's data: Mr. Frank Brittell (a retired, high-ranking law enforcement official), Mr. Richard Sutton (a private security consultant), and Mr. August Bequai, Attorney at Law.

Individual contributions of merit were made by Messrs. Richard Schechter of Lawrence Livermore Laboratory and Mr. John Heineke of the University of Santa Clara, who collaborated in the acquisition and analysis of considerable data on bank fraud and embezzlement, drug theft, and computer crime, as part of a contract with NMSS. As consultants to NRC, Messrs. Joseph Krofchek and Konrad Kellen of the Rand Corporation offered their expertise on various topics relating to the study.

Other individual contributions were made by Ms. Ellen Kraus, an NMSS consultant, who researched, reviewed and documented a host of open-source background material for the study and served as its senior editor; Messrs. Robert Chorba and Edward McKenzie of REHAB Group Inc., Falls Church, VA, contractors to NRC's Office of Administration, whose technical expertise facilitated computerization and analysis of the study's data base; and Ms. Mary Rodgers, whose hard work and patience as principal secretary are much appreciated.

Finally, we offer our sincere appreciation to the 30 federal government agencies and the 90 security experts in the private sector whose willingness to share with us their experience with insider crime and their opinions on methods for preventing such malevolence enabled us to amass a representative data base. Without their interest and cooperation, there would be no "Insider Study."

Although we are indebted to a host of contributors and advisors,* the final responsibility for the conclusions and views reflected in this study lies with the United States Nuclear Regulatory Commission, Office of Nuclear Material Safety and Safeguards, Division of Safeguards.

*Appendix A contains a list of some such contributors and advisors.

EXECUTIVE SUMMARY

Purpose

This study was undertaken in response to a Commission request of January, 1979. Its purpose is to determine, as logically and systematically as possible, the characteristics of potential insider adversaries to licensed fuel cycle facilities, transportation activities and reactors. In addition, it examines security system vulnerabilities that contribute to successful insider malevolence and assesses the relative effectiveness of some methods that have been employed to detect or prevent such malevolence.

Scope

The study addresses the two types of insider crime that are the primary concern of nuclear safeguards--theft and sabotage--and focuses on the "insider adversary," whose authorized access to a facility or activity may be exploited by him or others in the commission of a crime.

Method

In its initial request the Commission noted that the experience of analogous industries should be examined, but that "in collecting and analyzing such data from . . . non-NRC activities the staff should ensure that the relevancy and limitations of such data to NRC regulated activities are addressed." The study group relied primarily on data derived from analogous industries because the small number of cases of insider malevolence in the nuclear industry prohibited useful analysis. Nevertheless, the Commission's concern about the comparability of analogs was carefully considered. From an initial data base of over 200 apparently analogous cases of insider crime, the study group, using the general components of a nuclear safeguards system as a baseline, evaluated each case and assigned it an analog value based on the relative completeness and rigor with which the analogous safeguards system was designed.

After the case-by-case evaluation, the data base was reduced to 115 cases involving insider theft or sabotage in safeguards environments considered roughly comparable to the licensed nuclear industry.* Of the 115 cases, 45 are considered to have occurred in a "strong" safeguards environment with the balance occurring in a "weak" safeguards environment. Thirty-four cases involved conspiracies, 18 of which took place in a "strong" safeguards environment.

The study group's goal was not to rate analogous safeguards systems worse than, equal to or better than nuclear safeguards. Such a precise rating would have required measure-by-measure, item-by-item comparisons that were unattainable within the scope of the study. Of necessity, the study group has relied on the best analogs available for comparison.

Care should be exercised in drawing conclusions from the study due to difficulties in establishing comparability between nuclear and non-nuclear safeguards environments.

Limitations

The study's data base consists of insider cases wherein laws were broken or in which criminal intent was obvious, regardless of arrest or conviction. It includes examples of administrative and accounting discrepancies or irregularities only when proof of a crime existed.

It is possible that insiders whose crimes and identities went undetected have characteristics that are qualitatively different from those exhibited by the study's insiders, i.e., those whose crimes and identities were detected. In some instances, especially in the case of sabotage, we were unable to obtain statistics on a large population of incidents. The reader should be attentive to these limitations when interpreting tables and figures.

*Seven nuclear events are also included in the data base and integrated with the analog events for analytical purposes. Details on the nuclear events are contained in Appendix C.

Summary of Findings

The study revealed that malevolent insiders could be characterized to a certain extent based upon their objectives (i.e., theft or sabotage) and on the security environment in which they operated (i.e., strong or weak). As might be expected, group size and the level of organizational control exercised over the target (i.e., target control) seemed to affect an insider's method of operation. These and related findings are summarized in outline form below.

Characteristics of Typical Insider Thieves

- Acted alone.
- Were motivated by greed, indebtedness and financial inducement.
- Acted between their sixth and tenth years of employment.
- Planned their crimes well or moderately well.
- Relied on covert action.
- Used some type of equipment available on-site.

Characteristics of Typical Insider Saboteurs

- Acted alone.
- Were motivated by psychological problems, disgruntlement and revenge.
- Acted within two years of being hired.
- Acted on impulse.
- Relied on covert action.
- Used some type of equipment available on-site.

Characteristics of Insiders in a Strong Safeguards Environment*

- More conspiracies were formed.
- More reliance was placed on the use of non-routine access to the target in combination with covert action.
- Crimes were perpetrated later in the insiders' period of employment.
- Fewer insiders were coerced or induced into committing crime.

*As opposed to insiders in a weak safeguards environment. See p. 2-14.

Characteristics of Typical Insider Saboteurs

- Acted alone.
- Were motivated by psychological problems, disgruntlement and revenge.
- Acted within two years of being hired.
- Acted on impulse.
- Relied on covert action.
- Used some type of equipment available on-site.

Characteristics of Insiders in a Strong Safeguards Environment*

- More conspiracies were formed.
- More reliance was placed on the use of non-routine access to the target in combination with covert action.
- Crimes were perpetrated later in the insiders' period of employment.
- Fewer insiders were coerced or induced into committing crime.

Effect of Insider Thief's Target Control**

- Typical Thief with Operational Control
  - Relied on routine access to the target.
  - Relied on covert action.
  - Employed tactics involving subterfuge.
  - Was self-initiated, but was coerced or induced by other insiders or by outsiders about 20% of the time.
- Typical Thief with Policy/Management Control
  - Relied on routine access to the target.
  - Relied on covert action.

*As opposed to insiders in a weak safeguards environment. See p. 2-14.
**There were insufficient sabotage cases to permit determination of behavior patterns based on target control, which is defined as the level of organizational control exercised by the insider of the target of his crime.

- Employed tactics that involve manipulation of the targeted organizations' procedures and resources.
- Planned extensively.

- Typical Thief with No Target Control
  - Circumvented or defeated some type of access control in order to reach the target.
  - Relied exclusively on covert action.
  - Employed tactics involving subterfuge.
  - Conspired with other insiders and with outsiders.
  - Planned moderately well.

Comparison of Typical Single Thief vs Typical Theft Conspiracy*

SINGLE THIEF	THEFT CONSPIRACY
Type of Crime	**Type of Crime**
More often targeted mo[illegible] and information than mater[illegible]	. More often targeted material than information or money.
More often observed in weaker safeguards environment.	. More often observed in stronger safeguards environment.
Target Control	**Target Control**
More policymaker/manager involvement.	. More operational involvement.
Access	**Access**
Less reliance on non-routine access.	. More reliance on non-routine access.
Length of Service	**Length of Service**
Over one-third of crimes occurred in first 2 years of employment.	. Crimes rarely occurred in first 2 years of employment.
One-fifth of crimes occurred in 6-10 year period of employment.	. Over half of crimes occurred in 6-10 year period of employment.
Motivation	**Motivation**
Less often motivated by desire for money.	. More often motivated by desire for money.
Revenge, disgruntlement, psychological problems, game playing, ideology, sex and marital problems accounted for one-tenth of motivations.	. No conspiracies motivated by revenge, disgruntlement, ideology, etc.
Role	**Role**
Primary reliance on covert activity.	. Primary reliance on covert activity, but more overt activity than single insider.
Tactics	**Tactics**
Most often used guile, ruse and deceit; falsified documents/document manipulation; surreptitious removal; and abuse of trust.	. Similar to those used by single thief.

*There were insufficient sabotage cases to permit the same kind of comparison between the single saboteur and the sabotage conspiracy.

Security System Vulnerabilities to the Insider

The following vulnerabilities are those most frequently judged responsible for the success of the theft and sabotage cases in the data base and those most often cited by industry and government experts.

- Inconsistent application of security procedures.
- Failure to separate and rotate duties.
- Excessive trust due to longevity or position
- Personnel security deficiencies.
  - Inadequate screening.
  - Inadequate behavioral observation.
  - Poor management/employee relations.
- System design deficiencies (physical security or inventory controls).

Nuclear Safeguards Implications

Analysis of these vulnerabilities highlighted the following as practices to be avoided in the design and operation of nuclear safeguards systems.

- Allowing or making security exceptions to accommodate production quotas, deadlines, convenience, management pressure, public demand, or any other condition.
- Imposing security requirements that are unreasonably detrimental to production or profit.
- Improperly implementing or failing to implement the surveillance and rotation concepts, especially in material access areas and vital areas.
- Implicitly trusting management, persons in key positions (e.g., security officers, shift supervisors, material balance area custodians, control room operators), or any employee with many years of service.

Detecting Insider Malevolence

Analysis of our own study data plus review of other studies and expert opinion led us to conclude the following with respect to detecting insider malevolence within the nuclear industry.

- The role played by employees in insider crime detection is potentially significant and can enhance detection capability at nuclear activities if encouraged by management, perhaps by means of an intensive security awareness program. A healthy management/security/employee relationship might also catalyze employee aid in such detection. Also, a system of procedural overchecks by which theft and sabotage create obvious abnormalities can facilitate detection by a security-conscious workforce.
- Perpetrator absence was fairly significant in detecting bank fraud and embezzlement. Similarly, inventory manipulations designed to divert nuclear material at a fuel cycle facility might well be detected during an enforced absence (mandatory vacation period, for example, with facility access temporarily denied) during which necessary coverups could not be made by the perpetrator(s).
- The high success rates of audits/inventories and inspections against theft and sabotage respectively support the current use of these strategies in the nuclear industry. However, when such strategies are unannounced, randomly conducted and more frequently executed, they have proven even more effective in detecting the subtle, clandestine and complex acts of an insider adversary.

- Informants accounted for nearly 20% of all detections among the theft cases reviewed. To take advantage of this potentially fruitful strategy, it would be prudent for both NRC and its fuel cycle and transportation licensees to emphasize the provisions of the Atomic Weapons and Special Nuclear Materials Rewards Act, which provides a reward for information on the acquisition or export of special nuclear material (SNM) contrary to U.S. law. Also, licensee use of anonymous informant programs for reporting abnormalities might circumvent natural employee reluctance to bring unsubstantiated suspicions to the attention of management.
- The value of outsider awareness as a detection technique, especially for covert thefts by operational insiders and for conspiracies overall, suggests three implications for the nuclear industry:
  - Entities that receive the products of NRC's fuel cycle and strategic special nuclear material (SSNM) transportation licensees (primarily university and test reactors and the Department of Energy) can play a role in detecting insider crime at these licensees by being alert to any abnormalities associated with shipments and their contents.
  - NRC can play a role in detecting abnormalities associated with SSNM shipments by closely monitoring material accountability information.
  - A well-developed working relationship between licensees and local law enforcement, within the legal constraints that appertain, can be a productive channel for alerting licensees, NRC or the FBI to outsider awareness of improprieties at a nuclear facility or activity.

Insider Crime Prevention Strategies

The following conclusions about preventing insider malevolence in the nuclear industry were derived from analysis of insider case histories, other studies and expert opinion.

- Screening is an effective theft control strategy. Insiders who initially underwent screening based on a full-field background investigation or its equivalent, and subsequently became malevolent, tended to act alone rather than to become involved in conspiracies to commit theft.
- Although clearances cannot be expected to provide assurance of employee reliability after hire, when properly administered and based on well-defined and applicable criteria, they can reduce the likelihood that a nuclear activity will be infiltrated by criminal or terrorist elements or that it will hire (a) persons who misrepresent their identities or backgrounds; (b) persons with histories of criminality or emotional instability; or (c) persons who are susceptible to coercion or blackmail.
- A behavioral observation program in the nuclear industry can increase assurance of employee reliability after hire if: (a) employees' baseline "stable" behavior has been identified at the time of hire; (b) proper training is provided to supervisory personnel; and (c) its criteria are unambiguous and applied equitably.
- Psychological assessments, when designed and evaluated by professionals, can be an effective adjunct to screening and behavioral observation in the nuclear industry, but great care must be taken to prevent their misuse and mitigate their potential demoralizing impact on personnel.

- The use of preemployment screening, behavioral observation and psychological assessment does not obviate the need for strict internal procedural controls.
- An aggressive effort by the management of nuclear activities to (a) improve their rapport with the workforce, (b) provide support and direction to their security forces, and (c) foster in their employees an informed, healthy attitude toward security can improve the safeguards posture against the insider threat.
- Frequent internal inspections by operational personnel are the most effective way to prevent the success of an attempted sabotage.
- The best security against the insider threat in the nuclear industry is a dynamic and multi-faceted safeguards program, i.e., one that combines screening and assessment techniques, reliability programs, procedural control and security hardware. To be effective, such a program must be supported by management and applied uniformly to all personnel, including the safeguards staff itself, whose integrity is vital to nuclear security.

2. INTRODUCTION

2.1 Objective

On January 30, 1979, the Commission directed the staff to conduct a study of the potential threat to nuclear activities from insiders.* The objectives of the study are: (1) to determine, as logically and systematically as possible, the characteristics of the potential insider threat to fuel cycle facilities, transportation activities, and reactors (both power and non-power); (2) to examine actual security system vulnerabilities that contributed to successful insider malevolence; and (3) to assess the relative effectiveness of methods that have been employed to detect or prevent such malevolence.

2.2 Background

The background section contains information on two subjects: an earlier Division of Safeguards study of potential adversaries to nuclear programs and the threat definitions specified in Part 73 of Title 10 of the Code of Federal Regulations (Physical Protection of Plants and Materials).

*Memorandum by Samuel H. Chilk, Secretary, to Lee V. Gossick, Executive Director for Operations, Subject: "SECY-79-12 - Study of the Potential Threat to Nuclear Activities from Insiders."

2.2.1 Transition from Generic Adversary Characteristics Study

In June 1977 the NRC Office of the Secretary directed the staff to prepare a study of the characteristics of possible adversaries who might direct their activities against a nuclear facility. In response to this direction, the Office of Nuclear Materials Safety and Safeguards prepared and published the Generic Adversary Characteristics Study (GACS), NUREG-0459, March 1979.

The purpose of NUREG-0459 was to determine the characteristics of potential adversaries who might pose a threat to nuclear programs so that more effective safeguards systems could be designed to protect the industry against the malevolent acts of such adversaries, if ever attempted. The study was intended as an initial effort at threat definition.

After reviewing NUREG-0459, the Commission decided that "in light of the study's conclusions. . . regarding the significant reliance apparently placed on inside assistance by certain potential adversary groups, coupled with the general concern about insider threats," the staff should prepare "a more in-depth investigation of the potential insider threat to both SSNM facilities and transportation as well as to reactors."*

2.2.2 Current Threat Definitions

The threat characterizations below were established during public rulemaking by the Commission and based on: (1) earlier threat analysis by the NRC staff; (2) research by other government organizations and private contractors; and (3) public comment. Although the study group's efforts to characterize the potential insider threat are a continuation of earlier work, the group was not constrained by past analysis or assessments. The results of this study simply reflect the latest phase of continuing staff work to determine the characteristics of potential nuclear adversaries.

*Secretary memorandum, October 31, 1978.

2.2.2.1 Protection against Theft or Diversion of Formula Quantities of Strategic Special Nuclear Material (SSNM)

10 CFR Part 73.1(a)(2) contains the design basis threat that should be used by NRC licensees to design safeguards systems to prevent the theft or diversion of formula quantities of strategic special nuclear material by insiders: "an individual, including an employee (in any position)," and "a conspiracy between individuals in any position who may have (a) access to and detailed knowledge of nuclear power plants or the facilities referred to in Part 73.20(a) [SSNM facilities or activities], or (b) items that could facilitate theft of special nuclear material (e.g., small tools, substitute material, false documents, etc.), or both."

The external design basis threat for theft or diversion also incorporates inside assistance that may include a knowledgeable individual who attempts to participate in a passive role, an active role, or both.

2.2.2.2 Protection against Radiological Sabotage*

10 CFR Part 73.1(a)(1) specifies the following design basis threat for the design of safeguards systems to protect against radiological sabotage by insiders: "an internal threat of an insider, including an employee (in any position)." The external design basis threat for radiological sabotage also incorporates "inside assistance that may include a knowledgeable individual who attempts to participate in a passive role (e.g., provide information), an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), or both."

*"Radiological sabotage," as defined in 10 CFR Part 73.2, means any deliberate act directed against any plant or transport activity licensed by NRC or against a component of such a plant or transport activity that could directly or indirectly endanger public health and safety by exposure to radiation.

2.2.3 Other Considerations

2.2.3.1 General Impact of White-Collar Theft

The incidence of white-collar crime in this country is still rising with concomitant monetary and social costs to our society. This is reflected not only by dollar and property losses, but by loss of confidence and respect for private industry and government institutions.

Coping with problems caused by the growth of white-collar crime poses some perplexing problems for the federal government. How do you detect it without invading the privacy of individuals? Even when you detect it, the victim may be unwilling or unable to prosecute for fear of adverse publicity, cost of prosecution and even, in some cases, a risk to national security because of the information involved. This is not to say that this problem is being taken lightly. Both the Executive Branch and the Congress have taken actions to combat the encroachment of white-collar crime. The implications of these actions for the domestic nuclear industry are, as yet, undefined.

The response of private industry to the white-collar crime problem, as demonstrated by the results of the interviews conducted by our consultants, shows a marked range of expressed concern, from the "it won't happen to me" syndrome to the "I'd like to have good security, but it costs too much and will be too repressive" response. Also encountered was the intermediate position of "insurance

premiums are cheaper and less bother." It has become evident that many of these analogous industries are willing to tolerate some loss. In fact, many rely on the loss to trigger mechanisms to detect the crime. Yet how much of a loss can be tolerated by the domestic nuclear industry? The following statement by Herbert Edelhertz summarizes this dilemma well.

> ...we should not assume that a protection system has the capability to frustrate any reasonably foreseeable white-collar threat simply because it is very difficult to construct such a scenario; the history of white-collar crime is replete with successfully executed scenarios which would have been easy to write if hindsight were foresight.*

2.2.3.2 Proposed Clearance Rule

In March 1977, NRC published a proposed rule governing access to or control over special nuclear material (SNM) in the licensed sector.** The rule prescribes regulations instituting a clearance program for individuals with access to or control over SNM at power reactors, fuel processing plants and transportation activities. To determine these individuals' eligibility for access, their character, associations and loyalty would be investigated under standards established by the Commission. The program, which would be administered by NRC and paid for by its licensees, would involve only background investigations, not psychological screening.

As stated in the preamble to the proposed rule, "these regulations are being prepared to utilize a personnel security program as a measure to protect against those employed in the affected nuclear activities who might conspire to steal or divert special nuclear material or conduct sabotage which would endanger the public by exposure to radiation. Of course a clearance program itself does not

*Herbert Edelhertz and Marilyn Walsh, The White-Collar Challenge to Nuclear Safeguards (Lexington, MA: D.C. Heath and Company, 1978), p. 3.
**42 FR 14880, March 17, 1977.

entirely solve the problem of the 'insider' but in the opinion of the Commission, experience has shown that such programs do substantially reduce the risk of such conspiracies. Moreover, the proposed program is one of several elements in the Commission's overall safeguards program which together protect against threats, both internal and external."*

Following publication of the proposed rule, a public hearing was held in July 1978 to accommodate the opinions and views of the many people and organizations who commented on the rule in writing. The conclusions of the hearing board, which were published in April 1979,** led to separate consideration of clearance programs for reactors and fuel cycle facilities. A draft clearance rule for fuel cycle facilities only is now being considered by the Commission.

The results of the Insider Study, especially its findings on (1) the amount of preemployment screening undergone by the insiders whose crimes were analyzed, (2) inadequate screening as a security vulnerability, and (3) prevention strategies observed in use by analogous industries and government agencies, provide data relevant to consideration of the clearance rule and other regulatory actions designed to protect against possible malevolence by insiders.

2.2.3.3 Lawrence Livermore Laboratory Research

At the outset of the Insider Study, we learned that as a part of Lawrence Livermore Laboratory's (LLL) contract with NRC in the area of the material control and accounting (MC&A), it had been probing the attributes of insider adversaries. Its work was concentrated on bank fraud and embezzlement (BF&E),

*42 FR 14880.

**"Report of the Hearing Board in the Matter of Authorization for Access to or Control over Special Nuclear Material." Nuclear Regulatory Commission, Docket No. RM 50-7, Washington, D.C., 1978.

computer crime and drug thefts. Because the LLL research was relevant to our study, NRC tasked LLL to expedite and slightly reorient its effort and to produce an analysis of its insider-related information in direct suport of this study.*

Where appropriate, specific findings of the LLL report have been incorporated into the body of the study. Details on LLL's data sources and methodology and its most pertinent statistical results are contained in Appendix B.

2.3 Scope

2.3.1 General

The study analyzes the potential threat to licensed nuclear activities from insider adversaries. Its scope is threefold. First, it characterizes insiders involved in both nuclear theft and sabotage** and in analogous, non-nuclear theft and sabotage. Second, it analyzes the actual vulnerabilities of security systems that contributed to successful insider malevolence. Third, it examines the relative effectiveness of methods that have been used to detect and prevent such malevolence.

An "insider" is defined as a person who has authorized access to a facility or activity. The study focuses on the "insider adversary" whose authorized access may be exploited by him or others in the commission of a crime against that facility or activity. Insiders include owners, employees, contractors, consultants, contract security personnel, vendors, unescorted visitors, and janitorial staff.***

*For the complete LLL analysis, see NUREG-1234, "The Insider threat to Secure Facilities: Data Analysis." (to be published in June 1980).

**Appendix C contains details on the seven nuclear events in the data base; Appendix D contains a glossary of terms used in the study.

***Several cases involving former employees, who are technically no longer "insiders" but who may have information of significance to the access function, are reviewed in Appendix F to demonstrate the potential threat from that sector. Since, safeguards systems designed to protect against an external adversary would normally apply to such persons who have become, in fact, knowledgeable "outsiders," they are not included in the statistical data base.

2.3.2 Adversary Characteristics

The study examines the characteristics of the two types of insider crime that are the primary concern of nuclear safeguards: theft and sabotage. The insiders involved may have participated in an active or passive role; they may have worked alone, in collusion with other insiders, or in conspiracy with outsiders. Their actions may have been self-initiated, induced or levered by others, or unwitting.

We concentrated our reseach on case histories derived from (1) documented investigative, compliance or adjudicative records and (2) interviews with personnel involved in the prevention, detection, investigation or adjudication of insider incidents. Open-source literature was used only to the extent that it elucidated or amplified data acquired from the above sources. Data were gathered on 17 characteristics that relate to the (1) insider's position (e.g., length of service), (2) his behavior (e.g., motivations), (3) his resources (e.g., equipment), and (4) his method of operation (e.g., tactics).

2.3.3 Security System Vulnerabilities

In analyzing the vulnerabilities of security systems to insider malevolence, the study group attempted to determine, for every case reviewed, what weaknesses in the security system facilitated commission of the crime. Also, general perceptions on this issue were solicited from the security, investigative and legal personnel interviewed and from the consultants to the study. Generic system vulnerabilities applicable to nuclear licensees were extrapolated from these data.

2.3.4 Detection/Prevention Strategies

The study examines the effectiveness of methods used by government agencies and analogous industries to detect and prevent insider malevolence. The examination contained in Section 5 is based on three types of data. First, within the

incident data base, we identified the various methods that most often resulted in detection of the crime and collected information on preemployment screening. Second, the study group and its consultants sought opinions from their interviewees on various detection and prevention strategies vis-a-vis insider crime. Third, we reviewed several non-NRC studies and documents on the subject of techniques to prevent insider malevolence.

2.4 Limitations

2.4.1 Scope

The scope of the study was limited in the following ways:

(1) The insider crime data base contains only cases of theft and sabotage because these two types of crime are the primary concern of nuclear safeguards against insiders at the facilities and activities covered by this study.

(2) The data base consists of insider cases wherein laws were broken or in which criminal intent was obvious, regardless of arrest or conviction. It includes examples of administrative and accounting discrepancies or irregularities only when proof of a crime existed. Events arising from the occurrence of nuclear material inventory differences (IDs) are not included because AEC and NRC investigations of all large IDs have not established that special nuclear material has been stolen or diverted. (On the other hand, uncertainties in the material control and accounting techniques are such that possible successful theft or diversion in those instances cannot be conclusively ruled out.)

(3) With only three exceptions, data-gathering was restricted to domestic crimes because the relevance of foreign adversary actions to the domestic nuclear industry is uncertain and less is known about the safeguards required in analogous industries abroad.

(4) Evaluation of the effectiveness of current safeguards against the insider within the domestic nuclear industry is beyond the scope and mandate of the study.

(5) The purpose of the study is not to recommend changes to nuclear safeguards. Rather, it offers the Commission and NRC's licensees an analysis of the potential insider threat, security vulnerabilities to it, and means that have been effective in detecting and preventing it in analogous industries.

2.4.2 Data

The quality and amount of the data were limited in the following ways:

(1) The data base contains only cases in which the crime was detected and the insider(s) identified (although not necessarily arrested or convicted). It is possible that insiders who got away with theft or sabotage have characteristics that are qualitatively different from those exhibited by the insiders in our data base.

(2) In some instances, especially in the case of sabotage, we were unable to obtain statistics on a large population of incidents. The reader should be attentive to these limitations when interpreting tables and figures, each of which identifies the number of data points available for the calculations.

(3) Since the characteristics data are based upon the relative frequency with which specific attributes occurred within the data base of insider cases, they represent an estimate of the conditional probability that an insider will have a specific attribute given that he is malevolent. This is <u>not</u> equivalent to the conditional probability that an insider will be malevolent given that he has a specific attribute.

2.5 Sources

2.5.1 Analog Data

The major sources of analog data fall into two categories: U.S. Government agencies and private industry.* Thirty federal agencies were contacted personally; 16 of them provided case history data and 19 provided other information such as their views and opinions on insider crime. The Federal agencies, including military components, can be categorized as follow: investigative/adjudicative (8); regulatory (7); intelligence (5); production/R&D (5); personnel-related (3); and policymaking (2).

The case data they provided cover insider adversaries within their own agencies and the agencies over which they exercise control, as well as insiders in the industries they investigate or regulate.

Within the private sector, we interviewed 59 security officers (security managers, corporate security directors, etc.) of 30 different types of industries throughout the nation that were deemed analogous to the nuclear industry. These representatives, each with an average of 19 years of security-related experience, provided both case history data and expert opinion. The 30 types of industries can be categorized as follow: money handlers (6); material handlers, manufacturers, and distributors (18); money/material transporters (4); and other industries (2). Appendix E contains a list of these analogous industries by type.

Also interviewed were 31 state and local law enforcement officials, U.S. District Attorneys, private investigators and security consultants, and behavioral scientists.

*Some data (20 cases) were acquired from court records, from three private security investigators/consultants, and from four law enforcement agencies.

2.5.2 Nuclear Data

The sources of data on nuclear events were NRC, DOE and one private firm. These events, the only non-analogs in the data base, are described in detail in Appendix C.

2.5.3 Open-Source Data

Open-source literature was used to supplement previously obtained case histories and as a cue to cases for which documentation might be available among our sources. In no instance did we reconstruct a case solely on the basis of media reporting; a few cases were derived, however, from military counter-espionage training manuals, a banking trade publication, and a government document on cargo security. Nearly 300 security or insider-related articles, books, publications and documents from a variety of organizations, newspapers, journals, courts, and government and law enforcement agencies were reviewed as background during the course of the study. In keeping with the Commission's directive to make use of "relevant studies of the potential threats of insiders, both within the nuclear field and other areas where analogous situations may be present,"* we examined about a dozen government-sponsored and private studies, some of whose conclusions are referenced in Sections 4 and 5.

2.6 Approach

2.6.1 Use of Analogs

Because nuclear events involving insiders are too few in number to support meaningful analyses of the insider threat, we relied on an analog approach for both case histories and evaluations of expert opinion and other studies. This approach is based upon the assumption that a study of analogs can provide

*Secretary memorandum, October 31, 1978, p.3.

insight into the characteristics of potential insider adversaries to licensed nuclear programs. Except for seven nuclear events, all data and opinions in the study are derived from analogous cases and experiences.

2.6.2 Case Histories--Objective Data

2.6.2.1 Analog Development

Most of the study's data were derived from case histories of crimes committed by insiders in industries or activities that we considered analogous to the nuclear industry. After collecting over 200 such cases, we evaluated them to determine which ones were good analogs. This process involved examining several criteria as measues of analog value: value of the stolen or sabotaged material, risk to the perpetrator and public, consequences of the crime, etc. Value was discarded as a criterion because it is too relative a factor. Requiring comparability in risk and consequences was considered too restrictive because theft and sabotage of non-nuclear targets (drugs, money, classified information, aircraft, etc.) rarely involve risks or produce consequences as severe as could nuclear theft or sabotage. Instead, we concluded that an indirect criteria approach would be more appropriate. The most meaningful and objective indirect criteria were found to be the safeguards systems in place at the time of the crime and the extent to which they approximate those now required of NRC reactor, fuel cycle and transportation licensees. Thus, the more analogous the protective environment, the more analogous the case.

Recognizing the difficulty of comparing non-nuclear safeguards environments to those existing in the nuclear industry, we applied the following safeguards standards to each case and assigned it the analog value indicated:

Table 2.1

DEFINITION OF ANALOG VALUES

THEFT	Analog Value	SABOTAGE	Analog Value
Physical security and MC&A systems similar to those now required of NRC reactor, fuel cycle and transportation licensees	2 (Strongest Analog)	Physical security systems similar to those now required of NRC reactor, fuel cycle and transportation licensees	2 (Strongest Analog)
1) Either a physical security or an MC&A system similar to those now required of NRC licensees or 2) Both of these systems, but neither as well-structured or stringent as those required by NRC	1 (Weaker Analog)	Physical security systems in place, but not as well-structured or stringent as those required by NRC	1 (Weaker Analog)
1) Neither system in place or 2) Systems so inadequate as to preclude inclusion	0	1) No physical security system in place or 2) Physical security so inadequate as to preclude inclusion	0

After applying these criteria, we were left with 122 cases with analog value 1 or 2, including seven nuclear events,* which served as the analytical foundation for the study. Cases with an analog value of 0 were discarded and excluded from our analysis, except as noted below.

When we evaluated the original 200 cases, we discovered some unique aspects of insider crime among cases that became part of the analytic data base and among some cases that were discarded. To capture these rarely observed characteristics, we identified all such cases as "special cases" and examined their unique aspects in Appendix F.

*The criteria applied to the nuclear cases are the same as those applied to the analogs because the safeguards associated with them varied with the category and amount of material, the nation involved, and the date of the event. Nuclear cases did not automatically rate a value of 2.

To compensate for the lack of analogous sabotage data, we included in some of our sabotage analyses an additional 18 incidents whose safeguards analogy to the nuclear industry is tenuous (analog value 0), but which are representative of a pattern of saboteur behavior that is not contradicted by the cases with values 1 and 2. These 18 cases included several arson incidents and sabotage of military aircraft, grain elevators, a chemical storage site and an oil well. We will alert the reader to the inclusion of these special sabotage cases, throughout the analysis section.

2.6.2.2 Adversary Characteristics

From each of the 122 case histories, as well as the special sabotage cases, data were extracted on 17 characteristics of the inside adversary, his behavior, resources and method of operation. For most characteristics, such as group size, target control and length of service, the data were easily identified and measurable. For those that were not readily measurable, such as motivation and dedication, the data represent determinations based on the anlaysts' understanding of the entire case.

The characteristics were grouped into four categories that enabled us to analyze the insider threat from its nascent stage through actual commission of the crime.

The four categories are:

(1) Position-Related - those that characterize an insider within an organization or activity prior to commission of the crime

   (a) Target Control - the level of organizational control exercised by the insider over the theft or sabotage target

   (b) Screening - the quality of pre-employment screening undergone by the insider

   (c) Access - the type of access the insider had to the target as a function of his normal job duties

(d) Length of Service - the number of years of employment prior to commission of crime*

(e) Training/Skills - the level of training and skill possessed by the insider

(f) Training/Skill Relevance - whether the training and skills possessed by the insider facilitated commission of the crime

(2) Behavioral - those that characterize the insider's reasons for and willingness to commit the crime

(a) Stimulus - the action, agent or condition that incited the insider to crime

(b) Motivation - the incentive for the crime

(c) Dedication - the degree to which the insider was committed to accomplishing his crime

(3) Resource - those that characterize the support needed or used to carry out the crime

(a) Insider Group Size - the number of insiders involved in the crime

(b) Outsider Involvement - whether outsiders were involved in the crime

(c) Equipment Usage - whether any equipment was used in perpetrating the crime

(d) Equipment Availability - whether the equipment used (if any) was available within the victimized facility or activity

(4) Operational - those that characterize actual commission of the crime

(a) Crime Type - theft of money, material or information; or sabotage

(b) Role - whether the insider acted overtly or covertly

*Length of service refers to tenure with the targeted facility, not time in a particular job.

(c) Planning - the degree to which the insider prepared for the crime

(d) Tactics - the modus operandi of the insider

2.6.2.3 Security System Vulnerabilities

For each of the 122 cases, as well as the special sabotage cases, we identified the generic weakness(es) of the security system that facilitated commission of the crime. This determination was based on (1) vulnerabilities specified in documented cases, (2) statements of personnel involved in investigating or adjudicating the cases, or (3) analysts' knowledge of the security system in the victimized industries represented in the data base.

2.6.2.4 Detection/Prevention Strategies

For each case, we identified the means by which the crime was detected and the quality of the preemployment screening to which the perpetrator(s) was (were) subjected.

2.6.3 Expert Opinion--Subjective Data

To add perspective to the findings derived from the case histories, we sought expert opinion on system vulnerability and detection and prevention techniques. These opinions (supporting, opposing, or supplemental) were incorporated into the analysis. They were derived from (1) interviews with security, investigative and legal personnel; (2) studies by other government agencies, universities and security-related organizations; and (3) the store of experience in these areas amassed by our consultants.

3. ANALYSIS OF THE INSIDER ADVERSARY

Three sections comprise our analysis of the insider adversary. The first section contains implications for nuclear safeguards that we derived from the analysis. The second section contains a profile of the insider thief and behavior patterns associated with his crimes. The third section presents a profile of the insider saboteur. Figures and tables referred to in the second and third sections are contained in Appendix G.

3.1 Implications for Nuclear Safeguards

The threat posed by the insider is multi-faceted and can manifest itself in a variety of ways. What follow are implications of the insider threat that appear to have the greatest relevance for the domestic nuclear industry and its safeguards systems.

3.1.1 General

- Insiders rarely use weapons.
- Insiders rely primarily on routine access to reach their targets but on covert action to perpetrate their crimes.
- Most insiders had fair to good screening.*
- Most insiders are moderately to highly dedicated to perpetration of their crimes.
- Drug use or abuse was one of the more frequent motivations for the insider.

3.1.2 Insider Behavior in a Strong Safeguards Environment**

- More conspiracies were observed, but fewer involved outsiders.
- Equipment necessary for the crime was less often available at the site.

*See Sections 5.4.1 and 5.4.2 concerning the effectiveness of preemployment screening.

**As opposed to insiders in a weak safeguards environment.

- More reliance was placed on the use of non-routine access in combination with covert action, and more insiders with no control over the target were observed.
- Crimes were perpetrated later in the insiders' period of employment.
- Fewer insiders were coerced or pressured into crime.

3.1.3 Saboteur vs. Thief

The inside saboteur and inside thief behave differently in several respects and present different problems to safeguards designers.

- The saboteur is more often motivated by psychological problems, desire for revenge or disgruntlement than is the thief. Because these motivations may manifest themselves on the job, the saboteur may be more vulnerable than the thief to detection by means of behavioral observation for which baseline behavior and attitudes were established during preemployment psychological evaluation and interviews.
- Saboteurs are more likely to act alone, although conspiracies were formed to commit both theft and sabotage.
- The saboteur appears to be more impulsive, i.e., exhibits lower levels of planning.
- Saboteurs possessed higher levels of training and skills.
- Saboteurs relied more on covert action.
- The threat from the thief increases through the tenth year of employment, whereas the saboteur usually acts within two years of being hired.
- The thief is most often motivated by a desire for money and least often motivated by psychological problems. A vigorous background investigation and reinvestigation program may be more valuable than behavioral observation in detecting a financially motivated adversary.

- The thief is more likely to have external assistance and twice as likely to be involved in conspiracy.

3.1.4 Theft Conspiracies vs. Single Insider Thefts

- Conspiracies tended to form later in the insiders' period of employment (6-10 years), whereas over one-third of single insider crimes occurred within the first two years of employment.
- Conspirators had generally lower levels of screening.
- Conspirators relied more on non-routine access to the target.
- Desire for money motivated most conspiracies. No conspiracies were observed that were motivated by revenge, disgruntlement, ideology or marital problems. These motivations represent just over one-tenth of the single insiders' motivations.
- More instances of leverage were observed in crimes involving a single insider.

3.2 Insider Thief

3.2.1 Behavior Patterns

In this section, selected characteristics of the insider thief are compared to determine variations in insider behavior. Two characteristics, target control and group size, were particularly useful as baselines for comparisons, so the first set of comparisons compare and contrast the behavior of insiders who held different types of target control, and the second set identifies similarities and differences between insiders who acted alone and insiders who acted in conspiracy.

3.2.1.1 Target Control

In the following comparisons, policy and management types of target control have been combined. Therefore, each insider had either policy/management, operational or no target control. These three types of insiders will be compared

in terms of their motivation, access, role, stimulus, group size, planning, involvement with outsiders and tactics.

(1) Motivation - Table G.1 displays the more frequently occurring motivations for each type of target control. Motivations related to money (greed, financial inducement and indebtedness) accounted for approximately 75% of all motivations regardless of target control.

Generally, drug use and personal loyalty motivated the operational insiders and those with no target control more often than the policy/manager types. It should also be noted that the widest variety of motivations occurred among operational insiders.

(2) Access - Table G.2 displays the types of access used by insiders having policy/management, operational or no target control. Clearly, the insider with no control over the target was forced to rely on non-routine access. Non-routine access was used next most frequently by the policymaker/manager.

(3) Role - Table G.3 indicates that most insiders, regardless of their target control, rely on covert activity to commit their crime. However, all insiders with no target control relied on covert action.

(4) Stimulus - Table G.4 shows what percentage of each type of insider was stimulated to act by each of the four stimuli. Although the majority of each type of insider is self-initiated, operational types are more frequently induced by other insiders or an outsider to commit a crime.

(5) Group Size - Of the three types of target control, the policymaker/manager was least likely to enter into a conspiracy, whereas the insider having no target control was most likely to conspire with an insider who did exercise some control over the target.

(6) Planning - Table G.5 displays what percentage of insiders with each type of target control used low, moderate and high levels of planning. Policy/management types exhibited the highest planning level, whereas only 44% of the operational types and 4% of insiders with no target control had a high level of planning.

(7) External Involvement - Table G.6 shows what percentage of each target control type colluded with outsiders (one or more than one) and what percentage had no outside assistance. Insiders who had no target control relied on outside involvement most often--52% of the time. This compares with 37% and 36% for operational and policy/management types respectively.

(8) Tactics - Table G.7 presents the tactics most frequently used by each target control type. Falsifying documents/document manipulation, the use of guile, ruse and deceit, and surreptitious removal were common to all types of target control with insiders having no control relying on the latter two tactics more frequently. The policy/manager type used either false or falsified documents 26% of the time while operational insiders used them only 10% of the time, and insiders with no target control made no use of them at all. Surreptitious removal was the most frequently used tactic for operational and no target control types, whereas it was the third most frequent tactic employed by the policymaker or manager. A marked difference among the three target control types emerges when the tactics are grouped into those involving manipulation of the targeted organizations' procedures and resources (Table G.8) and those involving subterfuge (Table G.9). The policymaker/manager is most likely to use manipulation. The operational and no target control types are most likely to use subterfuge.

3.2.1.2 Group Size

Seven characteristics of the lone thief and thieves in conspiracy are compared below.

	SINGLE THIEF	THEFT CONSPIRACY*
1.	Type of Crime	Type of Crime
	. More often targeted money and information than material.	. More often targeted material than information or money.
	. Observed more often in weaker safeguards environment.	. Observed more often in stronger safeguards environment.
2.	Target Control	Target Control
	. More policymaker/manager involvement.	. More operational involvement.
3.	Access	Access
	. Less reliance on non-routine access.	. More reliance on non-routine access.
4.	Length of Service	Length of Service
	. Over one-third of crimes occurred in first 2 years.	. Crimes rarely occurred in first 2 years.
	. One-fifth of crimes occurred in 6-10 year time period.	. Over half of crimes occurred in 6-10 year time period.
5.	Motivation	Motivation
	. Less often motivated by desire for money.	. More often motivated by desire for money.
	. Revenge, disgruntlement, psychological problems, game playing, ideology, sex and marital problems accounted for one-tenth of motivations.	. No conspiracies motivated by revenge, disgruntlement, ideology, etc.
6.	Role	Role
	. Primary reliance on covert activity.	. Primary reliance on covert activity, but more overt activity than single insider.
7.	Tactics	Tactics
	. Most often used guile, ruse and deceit; falsified documents/document manipulation; surreptitious removal; and abuse of trust.	. Similar to those used by single thief.

*Insiders within a conspiracy tended to have similar characteristics.

3.2.2 Characteristics Profile

The theft profile examines the 17 adversary characteristics according to the groups and order outlined in the approach section i.e., position-related, behavioral, resource and operational characteristics (see Section 2.6.2.2). The profile is derived from 112 cases in the data base that involved theft of money, material or information. When a distinction occurs between analog 2 cases (strong safeguards analogy) and analog 1 cases (weaker safeguards analogy), it is brought to the reader's attention because we believe the analog 2 cases are better examples of potential threats to the nuclear industry.

Position-Related Characteristics

Six characteristics are associated with the insider's position within an organization: 1) target control, 2) level of screening, 3) access to the target, 4) length of employment, 5) training and skill level, and 6) the relevance of the insider's training and skill to the crime he commits. Each characteristic will be examined in turn.

(1) Target Control - Figure G.1 indicates that most insiders (68%) exercised operational control over the target of their crime, whereas managerial and policy-level insiders comprised 22% of the population. Approximately 10% of the insiders had no target control, but most conspired with other insiders who did. Figure G.2 compares analog 1 and 2 cases. A greater percentage of insiders held managerial or policy-level positions in the analog 1 cases than in the analog 2 cases. The most obvious difference between analog 1 and 2 cases is that the insiders with no target control appeared more frequently in the analog 2 environment.

(2) Screening - Approximately 86% of the insiders underwent some degree of screening, ranging from a check of references to a full-field background

investigation. Figure G.3 shows that 11% of the insiders passed a full-field background investigation or its equivalent. As was expected, a comparison of analog 1 and 2 insiders showed that 41% of the analog 1 insiders, compared to 83% of the analog 2 insiders, received fair to good screening.

(3) Access - Figure G.4 shows the distribution of types of access used by insiders. The majority (81%) relied on routine access to their target. Figure G.5 compares the types of access used in analog 1 and 2 cases. In the analog 2 environment, insiders resorted more often to non-routine access in the commission of a crime.

(4) Length of Service - Figure G.6 suggests that the threat from an insider in an analog 2 environment increases up to the 6 to 10 year period of employment, whereas in the analog 1 environment, the threat peaks in the 3 to 5 year period before diminishing in the 6 to 10 year period. Further, 60% of the insiders in analog 1 cases, compared to 33% of the insiders in analog 2 cases, committed their crimes within 5 years of being hired.

(5) Training and Skills - Figure G.7 shows a comparison between analog 1 and 2 training and skill levels. Although the training and skill levels in analog 1 cases are fairly evenly distributed, the analog 2 insider tended to have lower training and skills.

(6) Training and Skills Relevance - Training and skills acquired on the job by analog 1 and 2 insiders were relevant to the commission of the crime 91% and 80% of the time respectively.

Behavioral Characteristics

Three characteristics are associated with the inside adversary's behavior: 1) the stimulus to the insider, i.e., what impelled the insider to act, 2) the motivation that was the underlying incentive to act, and 3) the level of dedication possessed by the insider. It should be noted that the behavioral characteristics most reflect the analysts' subjective perceptions based on their understanding of each case.

(1) Stimulus - Figure G.8 shows the types of stimuli that acted upon the insider in analog 1 versus analog 2 cases. In both situations, most insiders were self-initiated, but more analog 2 insiders were self-initiated than analog 1 insiders (92% vs. 65%). Fewer analog 2 insiders were levered or induced to commit a crime, and no analog 2 insiders were unwitting participants.

(2) Motivation - Table G.10 shows the 10 most often identified motivations in a comparison of analog 1 and 2 cases. Money (greed, financial inducement and debt) was the most frequent motivation. After money, personal loyalty and drug use, particularly for analog 1 cases, were the most frequently occurring motivations. Table G.11 provides a complete distribution of all motivations observed.

(3) Dedication - Figure G.9 compares analogs 1 and 2 and the distribution for levels of dedication. Most insiders had moderate to high dedication. More insiders in analog 1 cases were highly dedicated.

Resource Characteristics

Four characteristics are associated with the resources required to commit the crime: 1) insider group size; 2) outsider involvement in the insider crime; 3) equipment used; and 4) equipment availability. Each characteristic will be examined in turn.

(1) Insider Group Size - Figure G.10 shows that 70% of the theft cases were committed by insiders acting alone, 20% of the thefts were committed by three or more insiders in collusion, and 10% of the crimes were committed by conspiracies of two insiders. Comparing the analog 1 and 2 cases (Figure G.11), the data suggest that stronger safeguards required the insider to conspire with other insiders more often. In 39% of the analog 2 cases, collusion was evident, compared with 23% of the analog 1 cases.

(2) Outsider Involvement - From Figure G.12 it appears that the insiders operating in a stronger safeguards environment (analog 2) tended to be less involved with outsiders than insiders working in a weaker safeguards environment.

(3) Equipment Used - In the majority of cases (85%), equipment was necessary in the commission of the crime. A wide range of equipment was involved and included real or forged documents, computers, forklifts, trucks, rubber gloves, property passes, a short-wave radio and wire cutters. Interestingly, the use of weapons was rarely observed.

(4) Equipment Availability - In most cases (87%), some or all the equipment was available at the location of the crime. In analog 2 cases, the insider had to obtain equipment not available at the location of the crime more often than did the insiders in analog 1 cases.

Operational Characteristics

Four characteristics are associated with the operational profile of the insider thief: 1) the type of crime committed, 2) the role (overt or covert) played by the insider, 3) the level of planning, and 4) the tactics used by the insider. Each characteristic will be examined in turn.

(1) Type of Crime - The theft profile is derived from 112 cases involving the theft of money, material or information. One third of the cases were money thefts, approximately half (51%) were material thefts, and the remaining cases (16%) involved the theft of information. All three types of theft were deemed analogous to the theft of SSNM because they represent the unauthorized removal of items that were physically protected, accounted for and controlled. The targets of theft of information were either classified documents (both government and contractor-held) or proprietary documents/data (designs, exploration data, marketing plans, confidential law enforcement data, etc.).

(2) Role - Figure G.13 indicates that most insiders act covertly when committing their crime. Figure G.14 compares analogs 1 and 2 and suggests that in the stronger safeguards environment, the insider must resort to covert actions more often than the insider in an analog 1 case. The analog 1 cases approach an even split between overt and covert activity.

(3) Planning - Over 80% of the insiders had moderate to high planning levels. In Figure G.15, however, the data suggest that analog 1 insiders rather than analog 2 insiders had higher-level planning.

(4) Tactics - Table G.12 identifies the seven most frequently used tactics by insiders and the percentage of analog 1 and 2 cases in which they were used.* The total number of data points, 265, reflects the fact that a combination of tactics were employed in nearly every case. For example, surreptitious removal (the most frequently observed tactic in both analog 1 and 2 cases) was often accompanied by guile, false documentation and illicit sales, and computer manipulation was often used in tandem with altered records. It

*For a list of all tactics observed, see Table G.13.

appears that the insider resorts more frequently to guile and misrepresentation of authority (included in the "other" category) in a strong safeguards environment, and that falsified and phony documentation, as well as computer manipulation, are more likely to be the modus operandi of insiders operating against a weaker security system. The high percentage of use of surreptitious removal in both situations reflects the fact that the final step in most thefts is removal of the stolen items from the site and emphasizes the importance of exit searches.

3.3 Insider Saboteur--Characteristics Profile

The sabotage profile is derived from a data base that is limited to 54 insiders who participated in a total of 28 cases.* It is limited for two reasons. First, more complete and meaningful data could not be identified or were not available to us. Second, acts of vandalism, i.e., acts that did not obstruct productivity, interrupt operations or endanger lives, were excluded from the study. Because the sabotage data base is limited and includes special cases, the reader should view the following analysis as a clue rather than a conclusion about the inside saboteur's characteristics.

The 17 insider characteristics are examined in the same order as they were presented in the theft profile.

Position-Related Characteritics

(1) Target Control - Figure G.16 displays the types of target control held by inside saboteurs. Most often, the saboteur had operational control of the target. The second largest group of saboteurs had no control over the target. The size of this latter group (29% of the population) supports

*The 18 special cases referred to in Section 2.6.2.1 are included for all characteristics except insider group size.

the argument that access should be a function of and limited to an individual's job duties.

(2) Screening - The levels of screening to which the saboteur was subjected are depicted in Figure G.17. Approximately 74% of the insiders received some sort of screening with 65% receiving fair to good screening. A full-field background investigation or its equivalent was conducted or a polygraph examination was administered on 39% of the population.

(3) Access - Most saboteurs (88%) had routine access to their targets as indicated in Figure G.18.

(4) Length of Service - Figure G.19 indicates that the majority of inside saboteurs act in the first two years of employment. This suggests that screening should be emphasized because employee bahavior patterns may not have been sufficiently identified in one or two years to permit the detection of an aberration.

(5) Training and Skills - The inside saboteur usually had moderate to high training and skill levels (Figure G.20).

(6) Training and Skills Relevance - For 71% of the insiders, training and skills acquired on the job were relevant to committing the act of sabotage.

Behavioral Characteristics

(1) Stimulus - Of the 31 inside saboteurs for which data were available, 93% were self-initiated to commit the crime. Two insiders (6% of the population) were induced to act by outsiders.

(2) Motivation - Figure G.21 displays the seven most frequently identified motivations of the inside saboteur. No single motivation dominated, but the combined motivations of psychological or personal problems, disgruntlement and revenge accounted for 54% of the population. Table G.14 provides a distribution of all motivations observed.

(3) Dedication - The levels of dedication among the insiders were fairly evenly distributed between low, moderate and high (Figure 3.22).

Resource Characteristics

(1) Insider Group Size - Figure G.23 shows the distribution of numbers of participants in the 10 inside sabotage cases with analog values of 1 or 2. Two cases involved two or more insiders and in eight incidents, the insiders acted alone.

(2) Outsider Involvement - In four of the 28 cases, outsiders were involved. Usually, the insider acted as an agent to an outsider who was intent on sabotage.

(3) Equipment Used - The insider saboteur required the use of some type of equipment in 96% of the cases. Equipment used included tools, metallic objects, explosives, 55 gallon drums and incendiary material.

(4) Equipment Availability - Equipment used was available at the site of the crime in 73% of the cases.

Operational Characteristics

(1) Type - All cases used in this profile related to some type of sabotage.

(2) Role - Most inside saboteurs (88%) acted covertly, although 12% of the insiders were able to commit their act in an overt capacity (Figure G.24).

(3) Planning - As depicted by Figure G.25, most insiders (78%) exhibited low to moderate levels of planning prior to committing sabotage.

(4) Tactics - Because, as was expected, the most common tactic (67% of the tactics used) was a direct attack on the target, we attempted to discern different types of attacks. Of the 52 tactics employed in the sabotage cases: 1) 40% involved the disabling of the target (an act of low level violence that rendered the target inoperative); 2) 14% involved arson; 3) 10% involved introducing a foreign object into the target that rendered it inoperative; and 4) 4% involved the use of explosives. The next most frequently occurring tactics after direct attack were: 1) guile, ruse, and deceit; and 2) surreptitious entry and exit. They accounted for 17.3% of the tactics used. Table G.15 contains a complete list of all tactics used and the frequency with which they occurred.

4. SECURITY SYSTEM VULNERABILITIES TO THE INSIDER

4.1 Introduction

For all but five cases in the data set, we identified the one or more generic weaknesses of the security system that rendered it vulnerable to the insider adversary. In some cases, the vulnerabilities were extrapolated from "lessons learned" critiques done by the regulatory authority or targeted facility; in some, the information was gleaned from interviews with security people involved in the cases; but in most incidents, the vulnerabilities were deduced from the events themselves. Other, non-case-specific information on the vulnerability question was supplied by consultants to the study as a product of their numerous interviews.

4.2 Implications for Nuclear Safeguards

The following implications with respect to the vulnerability of a nuclear activity to insider malevolence are derived from the next section:

(1) Allowing or making security exceptions to accommodate production quotas, dead-lines, convenience, management pressure, public demand, or any other condition increases the vulnerability of a nuclear facility to the insider threat.

(2) As a corollary to the implication above, imposing security requirements that are unreasonably detrimental to production or profit will cause honest employees to tolerate their circumvention for the good of the company.

(3) Improper implementation or failure to implement the surveillance and rotation concepts, especially in material access areas and vital areas, increases the threat of insider theft and sabotage at a nuclear activity.

(4) Implicit trust in management, persons in key positions (e.g., security officers, shift supervisors, material balance area custodians, control room operators), or any employee with many years of service will weaken a nuclear facility's safeguards posture against the insider.

(5) Efforts by NRC and its licensees to reduce the probability of attempted theft and especially sabotage will be attenuated to the degree that personnel security programs are not improved.

4.3 Analysis of Insider Cases and Expert Opinion

We identified five vulnerabilities that most frequently accounted for the success of the crimes in the data base and were most often cited by industry and government experts:

- o Inconsistent application of security procedures
- o Failure to separate and rotate duties
- o Excessive trust due to longevity or position
- o Personnel security deficiencies
- o System design deficiencies.

Each vulnerability is analyzed in turn in the following sections.

4.3.1 Inconsistent Application of Security Procedures

As the security manager of a major airline put it, "most high value losses are not system failures, but the failure of people to adhere to the system." When convenience, timeliness or supervisory insistence conflict with security procedures, the inclination to circumvent the rules will often be followed. "Once a prospective adversary learns the circumstances under which exceptions to the rule will be tolerated or go unnoticed, he can readily exploit such situations to his advantage," observed a LLL safeguards project staff member in his report for the study.* For example, in a bank fraud in which a loan clerk approved what turned out to be a fraudulent loan on the strength of his boss, the loan officer's, OK because "time was of the essence," the boss/perpetrator was clearly taking advantage of

*Richard Schechter, The Insider Threat to Secure Facilities - A Synopsis of Nine Interviews (Washington: U.S. Nuclear Regulatory Commission, NUREG/CR-1279, 1980), p. 4.

inconsistent application of procedures. A metallurgical employee who was able to remove gold cathodes and anodes from the site exploited the guards' inattentive exit searches and ineffective use of metal detectors.

One pitfall associated with this vulnerability is the tendency for a facility that has enjoyed a consistently good security record or whose management suffers from the "it'll never happen to me" syndrome to become complacent about enforcing security regulations. Overconfidence, according to one expert, is the "Achilles heel" of security. Another contributing factor is high turnover rates among supervisory personnel, which can result in an employee receiving repeated warnings from a series of bosses without ever being seriously disciplined. A last factor is employee tendency to be excessively loyal to supervisors.

4.3.2 Failure to Separate and Rotate Duties

This factor played a role in about 10% of the theft cases and was relatively more contributory when the perpetrator exercised policy or management control over the target. For example, the commercial accounts supervisor of a bank was able to perpetrate a $300,000 diversion with the assistance of several outsiders because he not only managed and took applications for such accounts, but had routine access to signature cards, blank checks, coding machines and documentation associated with each account's monthly statement. In another case, a jewelry store manager was able to steal $200,000 worth of jewelry over a one-year period because he sold, priced, and inventoried the store's merchandise and had access to the vault as well. He accomplished his scheme by increasing the prices of other items so that the audit would balance.

As in these cases, when a single employee can carry out all the steps required for a theft and its coverup or for sabotage, protection against the single insider has been severely degraded. Even when separation and rotation theoretically exist, their effectiveness, especially in a small facility, is often vitiated by the buddy system. Failure to randomize and rotate two-man pairings (dual custody) can breed the type of familiarity whose corrosive effect on security vigilance is a serious threat to safeguards assurance.

4.3.3 Excessive Trust Due to Longevity or Position

In nearly 15% of the thefts, insiders, especially those in policy or management level positions, exploited this vulnerability. It also came into play when the insider acted covertly, achieving his aim through guile and deceit. Further, as noted in the theft profile, 16% of the insiders who operated in the stronger safeguards environment had more than 10 years of service, 50% had been on the job for 6 to 10 years, and 17% occupied management or policy level positions. In a classic espionage case, for example, a lieutenant colonel assigned to the Office of the Joint Chiefs of Staff obtained documents containing defense secrets for the Soviet Union over a five-year period. A senior intelligence officer described by a former associate as "so patriotic," the colonel had been granted top secret and cryptologic clearances. Even after his retirement from the Army, he was made privy to classified information simply through visits with former military co-workers at the Pentagon. Clearly, excessive trust in this fellow officer and "patriot" who was "Army all the way" contributed greatly to his success as a spy.

The opinion was expressed that the tendency of managers to place too much trust in employees with tenure makes control of the insider threat especially difficult, whereas employees who place excessive faith in senior personnel simply due to their position may find themselves involuntary colluders or unwitting conspirators.

A number of our interviewees espouse a philosophy that in any but the security world would seem to border on paranoia, namely, "never trust anyone." It translates, however, to development of a safeguards system that is totally independent of the trustworthiness and integrity of the workforce, even of the "safeguardians" themselves, the system designers and security officers.

4.3.4 Personnel Security Deficiencies

Inadequate screening, insufficient behavioral observation and poor management/employee relations contributed to the success of about 15% of the theft cases but played a much greater role in sabotage incidents (72%). Also, the prevalence of inadequate screening and behavioral observation in situations where insiders were coerced or levered into theft collusion suggests that employers who are unaware of their employees' backgrounds (e.g., a previous arrest) or financial situations may be jeopardizing their security.

Inadequate screening was judged a vulnerability when it was discovered after the fact that the insider had a criminal record that made him a poor risk or that he had a history of emotional instability that cast doubt on his ability to function reliably. Insufficient behavioral observation was applied when the malevolent insider suffered from a psychological or personal problem (including drug abuse) that should have warned an alert co-worker or supervisor of potential difficulty. Poor management/employee relations refers to situations in which management failed to provide a mechanism for airing and resolving employee grievances, additional safeguards during a strike, or proper recognition and incentives for its employees, especially those in routinized and highly disciplined environments who may become frustrated and alienated.

The following cases exemplify these three deficiencies.

(a) A newly hired employee of an armored transport company was allowed to serve as truck custodian before completion of his background investigation. After he and an outside accomplice relieved the truck of $250,000, the company found that he had been convicted of armed robbery.

(b) A sailor who was convicted for sabotaging an aircraft carrier committed the arson, which caused $7.5 million damage, while suffering an LSD flashback. At his trial, he was also found guilty of possession and distribution of LSD and mescaline, both hallucinogens.

(c) At the Surry nuclear power plant, two control room trainees were arrested for vandalizing fresh reactor fuel. The two perpetrators claimed their attempts to bring safeguards deficiencies at the plant to the attention of the appropriate authorities went unheeded by management and federal inspectors.

4.3.5 System Design Deficiencies

As opposed to improper use of existing safeguards procedures and hardware, this vulnerability refers to deficiencies in safeguards system design. The very inclusion of a case in our data base implies a moderate to high degree of analogy to nuclear safeguards. Nevertheless, the targeted facilities or activities were occasionally rendered vulnerable to insider crime, especially theft, for want of one or two safeguards measures. The following examples illustrate such deficiencies.

(a) Two production workers and a janitor at a drug manufacturing company stole approximately $150,000 worth of antibiotics. At shift's end, the production workers would set aside a cannister containing the tablets inside the controlled area. The janitor, their accomplice, would then pick it up in his vacuum cleaner during a later shift. No search of janitorial equipment was made.

(b) Two uranium mill workers stole seven barrels of yellowcake worth $300,000. The site had no access controls to the yellowcake storage area, and its guards were stationed only at the main gate, with no roving patrols, despite the existence of other perimeter gates.

(c) A metallurgical reprocessing plant was bilked out of an undetermined amount of gold because it failed to inspect the scrap it received from an electronics company. A shipping and receiving manager at the electronics company, in collusion with an employee of the reprocessing plant, was substituting a foreign substance for some of the precious metal scrap, keeping the weight of the scrap consistent with the voucher, and signing the dispatch forms as authorized. His accomplice received and signed for the scrap at the reprocessing plant at which only weight measurements were required. They split the proceeds from the sale of the gold.

5. DETECTION AND PREVENTION STRATEGIES

5.1 Introduction

In its original mandate to the study group, the Commission asked that we "evaluate experience in analogous situations to assess the effectivity of methods or techniques for detecting or preventing insider threats...."* Our analysis in response to this request is based on data obtained by LLL and by us, non-NRC studies, and expert opinion.

5.2 Implications for Nuclear Safeguards

The following implications for detecting and preventing insider malevolence are derived from sections 5.3 and 5.4.

5.2.1 Detection

(1) The role played by employees in insider crime detection is potentially significant and can enhance detection capability at nuclear activities if encouraged by management, perhaps by means of an intensive security awareness program. A healthy management/security/employee relationship might also catalyze employee aid in such detection. Also, a system of procedural overchecks by which theft and sabotage create obvious abnormalities can facilitate detection by a security-conscious workforce.

(2) Perpetrator absence was fairly significant in detecting bank fraud and embezzlement (BF&E). Similarly, inventory manipulations designed to divert nuclear material at a fuel cycle facility might well be detected during an enforced absence (mandatory vacation period, for example, with facility access temporarily denied) during which necessary coverups could not be effected by the perpetrator(s).

(3) The high success rates of audits/inventories and inspections against theft and sabotage respectively support the current use of these strategies in the

*Secretary memorandum, October 31, 1978.

nuclear industry. However, when such strategies are unannounced, randomly conducted and more frequently executed, they have proven even more effective in detecting the subtle, clandestine and complex acts of an insider adversary.

(4) Informants accounted for nearly 20% of all detections among the theft cases reviewed. In order to take advantage of this potentially fruitful strategy, it would be prudent for both NRC and its fuel cycle and transportation licensees to emphasize the provisions of the Atomic Weapons and Special Nuclear Materials Rewards Act.* Also, licensee use of anonymous informant programs for reporting abnormalities might circumvent natural employee reluctance to bring unsubstantiated suspicions to the attention of management.

(5) The value of outsider awareness as a detection technique, especially for covert thefts by operational insiders and for conspiracies overall, suggests three implications for the nuclear industry:

   (a) Entities that receive the products of NRC's fuel cycle and SSNM transportation licensees (primarily university and test reactors and the Department of Energy) can play a role in detecting insider crime at these licensees by being alert to any abnormalities associated with shipments and their contents.

   (b) NRC can play a role in detecting abnormalities associated with SSNM shipments by closely monitoring material accountability information.

   (c) A well-developed working relationship between licensees and local law enforcement, within the legal constraints that appertain, can be a productive channel for alerting licensees, NRC or the FBI to outsider awareness of improprieties at a nuclear facility or activity.

*This 1974 Act provides for a reward of up to $500,000 for, among other things, information on the acquisition or export of SNM contrary to U.S. law.

5.2.2 Prevention

(1) Screening is an effective theft control strategy. Insiders who initially underwent screening based on a full-field background investigation or its equivalent; and subsequently became malevolent, tended to act alone rather than to become involved in conspiracies to commit theft.

(2) Although clearances cannot be expected to provide assurance of employee reliability after hire, when properly administered and based on well-defined and applicable criteria, they can reduce the likelihood that a nuclear activity will be infiltrated by criminal or terrorist elements or that it will hire: (a) persons who misrepresent their identities or backgrounds; (b) persons with histories of criminality or emotional instability; or (c) persons who are susceptible to coercion or blackmail.

(3) A behavioral observation program in the nuclear industry can increase assurance of employee reliability after hire if: (a) employees' baseline "stable" behavior has been identified at the time of hire; (b) proper training is provided to supervisory personnel; and (c) its criteria are unambiguous and applied equitably.

(4) Psychological assessments, when designed and evaluated by professionals, can be an effective adjunct to screening and behavioral observation in the nuclear industry, but great care must be taken to prevent their misuse and mitigate their potential demoralizing impact on personnel.

(5) The use of preemployment screening, behavioral observation and psychological assessment does not obviate the need for strict internal procedural controls.

(6) An aggressive effort by the management of nuclear activities to: (a) improve their rapport with the workforce; (b) provide support and direction to their security forces; and (c) foster in their employees an informed, healthy attitude toward security can improve the safeguards posture against the insider threat.

(7) Frequent internal inspections by operational personnel are the most effective way to prevent the success of an attempted sabotage.

(8) The best security against the insider threat in the nuclear industry is a dynamic and multi-faceted safeguards program, i.e., one that combines screening and assessment techniques, reliability programs, procedural control and security hardware. To be effective, such a program must be supported by management and applied uniformly to all personnel, including the safeguards staff itself, whose integrity is vital to nuclear security.

5.3 Analysis of Detection Strategies

5.3.1 Insider Cases

During the data-gathering phase of the study, we attempted to identify the method of detection for each insider crime examined. We focused on the initial means by which the crime was detected, not on determination of culpability.

The data in this section are based upon the relative frequency with which specific methods detected insider malevolence. Since all detection methods were not applicable to all cases in the data base, these frequencies reflect the

probabilities that the detection methods were effective, without consideration of whether they were employed. Therefore, methods that were frequently employed tend to appear more effective than they may, in fact, have been, whereas detection methods infrequently employed tend to appear less effective than they may, in fact, have been.

Figure G.26 compares the distribution of method of detection for theft and sabotage. The first six methods listed can be attributed to the security systems (MC&A, physical and personnel) at the targeted facility; the last five methods are not related to site security. The following definitions were used:

(a) Internal Audit/Inventory - audit or inventory undertaken as part of the victimized facility or site material control and accounting procedure

(b) Internal Inspection - inspection undertaken as part of the victimized facility or site security program

(c) Physical Security - CCTV, detectors, alarms, etc.

(d) Employee Observation - visual observation of the crime taking place by an employee

(e) Perpetrator Absence - crime detected due to the absence (leave, illness, death) of the perpetrator, usually because he/they were thus unable to continue coverup

(f) Employee Awareness of Abnormal Activity/Condition - suspicious situation or behavior reported by an employee

(g) Informant* - a tipster (insider or outsider) whose identity was not revealed

(h) Confession - perpetrator admission of the crime

*It is unknown whether informants were insiders or outsiders. Because structured informant programs were rarely in place within our analog industries, we included informants as a method of detection unrelated to site security systems.

(i) Investigation of Unrelated Activity - ancillary result of an investigation unrelated to the crime in question

(j) Outsider Awareness of Abnormal Activity/Condition - suspicious situation or behavior reported by an outsider; includes customer/client complaints

(k) External Audit/Inventory/Inspection - audit, inventory or inspection by an authority external to the victimized facility/site, e.g., regulatory inspection or bank examination

Except for employee observation, which is nearly as effective in both types of crimes, the methods that show high success rates for theft are much less successful against sabotage and vice versa. Overall, however, employee awareness of abnormal activity or condition was the clear leader for both types of crime.* When combined with visual observation of the crime by employees, the two methods account for 28% of theft detection and 61% of sabotage detection.

Although perpetrator absence was one of the two least successful methods observed in our data set, its effectiveness was more significant among the bank fraud and embezzlement BF&E cases researched by LLL.

Informants played a significant role in theft detection and no role in sabotage detection. This may be because theft is more likely to involve collusion than sabotage.

For sabotage, the high degree of effectiveness of techniques related to site security systems is clearly indicated. For theft, on the other hand, site detection mechanisms were 40% less effective. To determine to what degree

*For sabotage, this may be somewhat misleading since an act of sabotage will sooner or later come to the attention of someone, most logically another employee. In only two of these cases was employee detection sufficiently timely to prevent serious damage. On the other hand, an act of sabotage may be more likely to be reported by other employees, who may suffer physically or financially from its consequences, than is theft, which affects other employees less personally.

the lower effectiveness of site security systems in detecting theft depends on the overall strength of the security system, we further subdivided the theft data into analog 1 and 2 cases (Tables G.16 and G.17 respectively). A comparison between the two tables suggests that, as expected, the stronger the site safeguards system (analog 2), the more one can rely on it to detect insider theft.

From Table G.18, which compares detection method effectiveness conditional upon the target control of the perpetrator for theft and sabotage, we derived the following obervations:

(1) In the case of theft, no matter what the target control of the perpetrator, detection mechanisms unrelated to site security were overall more effective than mechanisms related to site security. Nevertheless, internal audits and inventories remain the most effective detection method for every level of perpetrator.

(2) Although internal inspection is the second most successful method of detecting sabotage overall, it appears totally ineffectual when a manager or policy-level insider is involved.*

LLL's study of bank fraud and embezzlement (BF&E) cases (Appendix B, Table B.8) contradicts Table G.18's data with respect to the relative effectiveness of internal and external audits/inventories, possibly because of the homogeneity of its data set. In the BF&E cases, executive and top management perpetrators were more likely to be caught by means of outside bank examinations than by internal audits, whereas low/middle management and staff were much more likely to be detected in an internal audit. LLL stated that this accents the lack of independence between internal auditors and the top officials of the bank.

*This result may not be as significant as it first appears due to the small number (five) of managerial and policy-level saboteurs.

On the other hand, the BF&E cases support our findings that, in theft, outsiders are more likely to aid in the detection of operational staff than policy/management level personnel, probably because the amount of interaction with the public decreases with position.

The distribution of method of detection, conditional upon the role of the insider, is portrayed in Table G.19. Table G.19 reveals that both overt and covert theft are detected in nearly equal proportion by techniques related to site security and by those not related to site security. However, as might be expected, the data reveal a slightly greater degree of effectiveness against overt theft for techniques related to site security.

Table G.20 compares the method of detection for theft and sabotage given that the perpetrator was a single insider or a conspiracy of insiders.* For theft, the higher the number of insiders, the more effective were both internal and external audits and inventories. Presumably, this reflects the fact that as more insiders become involved in the crime, it becomes more likely that one of the conspirators will overlook a manipulation necessary to the coverup.

Although confession was effective in only 5% of our theft conspiracy cases, it was the likeliest method of detection of large conspiracies (five or more) in the BF&E cases. LLL speculated that as group size grows, it becomes increasingly likely that an individual will become involved with the group who is less able to withstand the tensions associated with accounting coverups.

When insiders conspired with outsiders to commit theft (Table G.21), both internal and external audits and inventories were considerably less effective than when

*Cases involving outsiders in collusion with one or more insiders are excluded from this table.

insiders conspired with insiders. In insider/outsider theft conspiracies, the outsiders were usually passive participants, often only providing financial inducement. Thus, the audits and inventories were actually detecting the acts of the insider participants, who were usually only one or two in number. Informants and unrelated investigations accounted for many more detections in insider/outsider conspiracies than in insider/insider conspiracies, probably because outsider involvement offers far greater opportunity for external mechanisms to play a role in crime detection.

5.3.2 Non-NRC Studies and Expert Opinion

This section contains information on insider detection that was derived from a study done under contract to NRC and from our interviewees and consultants.

In their work entitled The White-Collar Challenge to Nuclear Safeguards, prepared under contract for NRC, Herbert Edelhertz and Marilyn Walsh of the Battelle Human Affairs Research Centers offer considerable insight into the susceptibility of white-collar nuclear theft* to detection and the probability of an insider thief being detected.

After observing that susceptibility to detection is an adversary attribute determined by the safeguards system but assessed by the adversary in terms of his potential for success, they note that

> Because the white-collar adversary...will be something of an expert on his susceptibility to detection, attempts to deter adversaries by creating a facade of system detection capabilities are unlikely to be successful.**

*They define nuclear white-collar crime as "illegal act or series of illegal acts committed by non-physical means and by concealment or guile, to steal or divert nuclear materials or to otherwise deprive nuclear regulators/agencies or licencees [sic] of information necessary to achievement of safeguards objectives." Herbert Edelhertz and Marilyn Walsh, The White-Collar Challenge to Nuclear Safeguards (Lexington, MA: D.C. Heath and Company, 1978), p. 2.

**Ibid., p. 34.

They recommend that nuclear safeguards planners direct their detection efforts to "multiplication of the number and level of those points at which detection can occur" and "consistent, timely, and imaginative use of detection mechanisms already available."* These approaches would be more effective, they feel, than "trying to achieve a degree of system sensitivity that makes all participants equally and highly detectable or attempting to 'impress' employees with noncredible detection powers."** They are strong advocates of consistency and timeliness in invocation of a detection system response, observing that such a response will enhance the system's sensitivity, reduce the amount of malevolence it will tolerate, and increase the adversary's susceptibility to detection.

Edelhertz and Walsh then offer the following propositions as descriptors of insider adversary susceptibility attributes:

> Given similar and adequate access attributes, the white-collar adversary with authority to correct, verify, edit, and/or reconcile discrepancy or error will be relatively less susceptible to detection than are those whose work he monitors.
>
> Given similar and adequate access attributes, the white-collar adversary performing a function(s) in which the expectation of error or discrepancy is great will be relatively less susceptible to detection than one performing in an area where error expectation is small.***

With respect to the second proposition, the authors note that the measurement limitations of current nuclear technology are such that "the expectation of some discrepancy and/or error...within a process period is both real and reasonable, and therefore represents a weakness than can be exploited,"**** especially by one who works in such an environment and who knows well the allowable material accountability tolerances of his facility.

---

*Ibid.
**Ibid.
***Ibid., p. 36.
****Ibid., p. 37.

The authors claim that the following attributes of an insider adversary's actions negatively affect the capability of a nuclear safeguards system to detect them:

(1) Subtlety - his actions are likely to be indirect and not overtly inappropriate in nature (i.e., likely to conform to business as usual or standard operating procedures)

(2) Clandestine Nature - inherent success of his actions depends on their not being detected, upon their being misinterpreted, or upon their being discovered so long after their occurrence as to be untraceable to him

(3) Complexity - his actions may be intricately conceived, planned and implemented and they are usually executed within a closed system (i.e., a licensed nuclear facility) whose strict procedures, controls and tolerances encourage elaborate manipulations.*

Finally, Edelhertz and Walsh address some factors that affect the probability that a safeguards system will detect insider nuclear theft and its perpetrator:**

(1) Number of Checks on an Adversary's Work - An adversary's probability of detection increases as the number of checks on his activities increases only if some or all of the checks are totally independent of reliance on his work and some or all of the checks occur within functional areas or subsystems over which he has no control.

(2) Frequency of Checks Made - The frequency of checks over time, and their frequency in relationship to one another, may increase the likelihood of detection given that they are ordered, scheduled, and implemented in a manner sufficiently independent of a potential adversary.

*Ibid., p. 63 ff.
**Ibid., p. 37 ff.

(3) Content and Sufficiency of Checks - The white-collar adversary is greatly aided by verification procedures that are routinized and essentially perfunctory in nature. Thus, no matter how many or how frequent checks on a potential adversary are, they must be of sufficient content and substance.

(4) Rigor of Adherence to Procedure - Verification, checking and safeguards procedures that are stringently, consistently and without fail required of everyone, every time, and in every place will increase the probability of detecting a white-collar crime and its perpetrator.

A number of the security experts we interviewed offered views on the effectiveness of detection techniques. Among their opinions, one was widely held: a thorough audit by a team that is completely independent, not only of the operation being audited, but of the company itself, is an excellent detection device.*

To the extent that such audits are unannounced and frequent, their value is enhanced even more. As one of the consultants to the study observed, the effectiveness of audits in the cases he reviewed "was denigrated by the normally long time lag between commission of the act and detection."**

Several industries we contacted, including two metallurgical firms, an auto manufacturer, a department store, a bank and an aerospace company, stressed the value of anonymous informant programs (sometimes with reward incentives) to encourage tips about insider crime. Although one security consultant interviewed believes that reward programs are counterproductive because they are detrimental to employee morale, their effectiveness in a number of analog industries cannot be disputed.

*Such a technique has obvious deterrent value as well.

**Richard Sutton, Jr., "Insider Threat Survey of Analogous Private Industries" (Washington, 1979), p.4.

One U.S. intelligence agency interviewed operates an effective, informal "informant net" by means of a staff security officer program. In this program, a trained employee in each major organizational component serves as an operational adjunct to the agency's security office.

In a supplemental report prepared for the study by LLL, a thorough security education program was recommended as a valuable means of integrating nuclear employees into the security monitoring process. This opinion was echoed by a number of security experts who rely on loyal, sensitized employees to augment procedural and technical detection methods.

With respect to detection by means of physical security, one source cited the successful use of pinhole cameras that are hidden in the wall and activated by means of a trigger mechanism whenever a sensitive operation is performed. CCTV, he noted, is best employed as a detection mechanism where it cannot be seen by workers.

One interviewee, the corporate security director of a major auto manufacturer with 29 years of security experience, observed that "certainty of detection is the best deterrent." This belief is borne out by the results of a 1979 study of employee theft by the University of Minnesota Department of Sociology.* The

*John P. Clark, et. al., Theft by Employees in Work Organizations - A Preliminary Final Report (Minneapolis: University of Minnesota, Department of Sociology, prepared under grant from the U.S. Department of Justice, 1979), p.5. This work was of particular interest to the study group because, unlike our study, it contains characteristics data on "successful" insiders, those who have stolen or are now stealing from their employers without being detected, as well as characteristics data on employees who have never stolen (or do not admit to ever having stolen) from their employers. This information was derived from questionnaires sent to a random sample of nearly 10,000 employees at all occupational levels in 35 firms in the Minneapolis area. The study balances these employee data with data derived from interviews with more than 180 executives from these same firms who furnished information about a variety of managerial perspectives and practices regarding theft by employees within their respective organizations.

study found that among the nearly 5000 anonymous respondents (retail, electronics manufacturing and hospital employees) to a questionnaire devised for the study, the most consistent predictor of theft involvement was the employee's perceived chance of being caught. In companies where the respondents indicated there was a significant probability of being caught if they stole something, less theft was found.

5.4 Analysis of Prevention Strategies

5.4.1 Insider Cases

We indicated in our analysis of detection strategies (see p. 5-6) that in only two cases of sabotage was employee awareness, which is a generally good method of detecting sabotage, sufficiently timely to prevent serious damage. On the other hand, internal inspection, another good means of detecting sabotage, does appear to be successful at preventing successful sabotage. Internal inspections accounted for a full two-thirds of the cases in which the act was discovered in time to avoid serious damage. For example, several instances of aircraft and ship sabotage involving damage to vital components were detected during routine, pre-deployment inspection checks. Although some financial loss was incurred in these cases, more serious, post-deployment results in terms of crew safety were prevented.

As noted in the theft and sabotage profiles, data were gathered on the level of preemployment screening to which the insiders were subjected. The standards used for evaluating screening are defined in Figure G.3. The application of these standards entailed judgment on the part of the analysts as screening procedures rarely fit neatly into one category or another. Once a judgment was made, however, we applied it consistently to similar types of screening.

Table G.22 shows the distribution of insider group size, conditional upon the level of screening for theft. Two observations may be drawn from this table:

(1) Malevolent insiders who underwent good preemployment screening were significantly less likely to conspire with other insiders than were those who received lesser levels of screening.

(2) Screening at <u>any</u> level less than good did not have a statistically significant effect on conspiracy formation.

Thus, the highest level of screening observed appears to reduce the probability of theft conspiracy formation, whereas all other levels do not.

The sabotage data in Table G.23 begin to display the same pattern as that which emerged from the theft data, but the small size of the sample causes fluctuations that prevent us from drawing statistically significant conclusions about the effectiveness of screening in preventing the formation of a sabotage conspiracy.

Table G.24 presents a distribution of lengths of service conditional upon level of screening for theft and reveals that the better an insider's screening, the less likely he is to perpetrate his theft within the first five years of employment. Also, nearly 70% of the thefts committed by insiders who were not screened at all occurred during the first five years of service. Although not reflected in the table, it is worth noting that <u>no</u> insiders with good screening committed their crimes during the first year of employment.

5.4.2 Non-NRC Studies and Expert Opinion

In the next five sections, the following prevention strategies are discussed and analyzed:

- o Preemployment screening and clearances
- o Behavioral observation programs
- o Psychological assessment techniques
- o Management-employee, management-security and security-employee rapport
- o Other prevention strategies

5.4.2.1 Preemployment Screening and Clearances

Unyielding advocacy characterized the opinion of many security experts on the issue of preemployment screening. One expert, with 30 years of federal law enforcement and private security experience with a major aircraft corporation, put it this way: "the basic answer to the insider threat is to be found in proper personnel selection." Several interviewees observed that today's lower moral standards and relaxed codes of ethics heighten the importance of personnel screening.

Even more inexorable was the widely held belief that federal and state restrictions on background investigations are choking security in private industry. As one expert, the security director of a major bank, put it: "government restriction on background investigations is the single most detrimental factor in controlling employee criminal misconduct." Several interviewees whose companies are under contract to the federal government observed that government clearances, for which background investigations can be more detailed and thorough, offer greater assurance of successful screening than privately conducted investigations, which are constrained by law.

Some experts offered the opinion that, given the critical nature of nuclear-related jobs, the nuclear industry should be exempt from such restrictions. Based on his interviews for the Insider Study, one of our consultants observed in his final report that "the nuclear industry cannot afford to be hamstrung by obstructive legislation, however noble the intent of that legislation."* He

*Frank Brittell, "Survey of the Insider Threat to the Nuclear Industry" (Los Angeles, 1979), p. 8.

further remarked that some precedent exists for this exemption authority--the banking industry has access to arrest and conviction records on applicants because banks are federally insured. "Surely," he pointed out, "security at a nuclear facility is equally important!"*

Although our interviews revealed strong general support for preemployment screening, several experts were quick to observe that, government restrictions notwithstanding, screening has inherent pitfalls. For example, some of the information acquired during a background investigation may be erroneous or misleading because:

(a) Previous employers who want to eliminate a problem employee may recommend him even, it appears, if he has been involved in malfeasance;

(b) Employers are reluctant to provide information of a derogatory nature about a previous employee since so doing can serve as the basis for a costly libel or slander suit against them;

(c) Employment records may not reflect earlier misconduct since some businesses, fearing adverse publicity, often allow employees who have committed a crime to resign quietly;

(d) Criminal conviction may not give a true accounting of an incident since plea-bargaining often results in reduction of the charge to a lesser offense; and

(e) A large proportion of white-collar criminals are never caught at all and thus go through life with perfectly clean records.

Finally, it is generally admitted that screening is a <u>preemployment</u> tool that does not assure <u>future</u> trustworthiness because any number of factors may impair stability and reliability after employment.

*Ibid.

In his report for the study, Richard Schechter, a member of LLL's safeguards project staff, offers for Commission consideration several reasons why clearances alone should not be expected to guarantee employee honesty in the nuclear industry.*

(a) The presumed value of a security clearance is based largely on the assumption that trustworthiness is an inherent quality, whereas to a large extent, it is a controllable variable that is conditioned by both the security system and operational management.

(b) The criteria that legitimately can be used to screen prospective employees may be irrelevant to conspiracies motivated by "principle" (e.g., insiders who wish to draw attention to poor security or who develop an anti-nuclear sentiment**); ethnic sympathy (e.g., one who rationalizes assistance to a foreign nation in nuclear theft because of ethnic ties); or management cover-up (e.g., unintentional abetting of a diverter by management which, for fear of NRC-imposed penalties, conceals an inventory difference or improper procedures).

(c) Clearances would have little value in a situation in which an honest employee was unwittingly duped into collusion by his co-workers or supervisors (e.g., an employee who "bends the rules" as a favor to his boss, only to find himself party to a theft with strong disincentive for reporting the incident).

*Schechter, pp. A7-A15.

**In discussions with representatives of the West Germany nuclear industry, LLL was informed that Germany considers the number one threat to its nuclear safeguards to be the "principled insider" who wishes to discredit Germany's nuclear industry by proving it vulnerable to theft of SNM.

Mr. Schechter avers that the aforementioned considerations are "by no means intended to argue that a security clearance is totally without value,"* but that security clearances can only be effective when they are supplemented by strict controls and periodic monitoring of employee conduct. He believes that clearances have potential value in the following areas:

(a) Eliminating candidates with strong criminal backgrounds, those who are susceptible to blackmail and who have a history of drug abuse or alcoholism, and those with backgrounds of psychological instability;

(b) Decreasing the ease with which a facility or activity could be infiltrated by a terrorist group or criminal organization; and

(c) Strengthening the deterrent to post-employment malevolence through threatened loss of clearance.

A 1978 study by Science Applications, Inc. (SAI) entitled Protection of Nuclear Power Plants against Sabotage by Two Insiders addresses the effectiveness of employee screening in defeating a two-insider sabotage attempt during the preparation phase (i.e., before entering vital areas to misuse/disable vital systems):

> Employee screening programs can be effective in identifying potential employees whose backgrounds indicate that they may possess the motivation to commit an act of sabotage (i.e., membership in subversive organizations, criminal records, a history of mental illness, etc.).**

SAI's conclusion that "the effectiveness of [screening]...may increase as the number of insider adversaries increases"*** is supported by the report of NRC's 1978 MC&A Task Force, which states that

*Schechter, pp. A6, A15.
**L. Kull, et al., Protection of Nuclear Power Plants against Sabotage by Two Insiders (La Jolla, CA: Science Applications, Inc., prepared under contract to Brookhaven National Laboratory, 1978), p. 49.
***Ibid., p. 53.

> ...there seems to be a conspiracy size at which the optimum safeguards program would change from primary reliance on procedural and technical safeguards against collusion with secondary reliance on clearances to primary reliance on clearances with secondary reliance on procedural and technical safeguards.*

Mr. Schechter takes issue with the Task Force's conclusion. Citing his aforementioned objections to the sole use of clearances to defeat conspiracies, he argues that

> ...there is no conspiracy size at which the optimum safeguards program would shift from primary reliance on procedural and technical safeguards to primary reliance on clearances! In fact, should any trade-off point exist, it would probably be between primary reliance on internally monitored controls for small conspiracies, and primary reliance on externally monitored controls for large conspiracies (which are particularly likely to involve high-level management).**

The screening conclusion in the previously referenced University of Minnesota study on theft by employees is of particular interest because many of its nearly 5000 anonymous respondents have committed or are committing theft without being detected by their employers. Also, the University had access to overall screening and misconduct records for each of the 35 companies involved in its survey. Its data suggest that "pre-employment screening of prospective employees continues to be an effective theft control strategy."*** The study further observed that "...a thorough pre-employment screening process indirectly conveys the message... that the organization is concerned with insuring the highest level of integrity among its workforce."****

*U.S. Nuclear Regulatory Commission, Report of the Material Control and Material Accounting Task Force, vol. 3 (Washington: U.S. Nuclear Regulatory Commission, NUREG-0450, 1978), p. VI-59.

**Schechter, p. A16. See also Tables B.2 and B.3 in Appendix B.

***Theft by Employees in Work Organizations, p. 7.

****Ibid., p. 8.

Several of the experts interviewed recommended personal, structured interviews as an effective means of evaluating an applicant's stability, attitudes, maturity and character.

The last study we reviewed that addresses screening efficacy was done by the Battelle Human Affairs Research Centers, Seattle, under contract with Sandia Laboratories, Department of Energy (DOE). The Role of Security Clearances and Personnel Reliability Programs in Protecting against Insider Threats, completed in 1979, evaluates the usefulness of existing security clearances in minimizing the potential insider threat to DOE-held SNM or information pertaining to it. Its data sources were Department of Defense (DOD), DOE and the Atomic Energy Commission.

After reviewing the history of government security clearance programs (initially designed to assess loyalty, extended to include reliability and trustworthiness, and now used by DOE to guard against misuse of SNM) and their implementation by DOE and DOD, the study examines assumptions underlying clearances and concludes that

> ...some of the motivations for compromise [of SNM] are explicitly included in security clearance criteria and some are not. Therefore, one would expect that...security clearances would be predictive of the insider threat only to the extent that clearance criteria represent or measure the "major" or "most important" motivations for illicit activity. Since it is possible to postulate many motivations for an employee to compromise SNM which are not represented as part of established clearance criteria, it is logical to conclude that security clearance procedures assess only a subset of all criteria which may be important in mitigating insider threats.*

It also observes that the absence of precise definitions for derogatory criteria introduces additional variance into the process.

*Ronald Perry et al., The Role of Security Clearances and Personnel Reliability Programs in Protecting against Insider Threats (Seattle: Battelle Human Affairs Research Centers, prepared under contract to Sandia Laboratories, 1979), p. 37.

In summarizing the efficacy of the clearance strategy against compromise of SNM, Battelle states that

> As presently structured, clearances are one kind of personnel screen which lack sufficient selection/elimination criteria reflecting behaviors predictive of insider threats and should not be considered useful in substantially mitigating such threats.*

The authors marshall several arguments to support this conclusion. First, they consider it unreasonable on statistical grounds to expect clearances to predict behavior (i.e., compromise of SNM) that is not represented by the criteria. Second, from an operational standpoint, clearance criteria use general measures of unreliability (e.g., disgraceful conduct) to predict specific behavior (e.g., diversion of SNM). Third, clearances used to assess insider threats rely on a prediction strategy under conditions that attenuate predictive capability (e.g., measuring past behavior and making predictions in a different context and making predictions that are expected to remain accurate over at least five years.)

Battelle admits that clearance programs are of use in general loyalty screening, but declares that "they cannot reasonably be expected to deal with insider threats."**

Although not subject to empirical treatment, the belief that clearances have pre-application deterrence value is widely espoused in the intelligence community. The knowledge that a full-scale background investigation will be conducted may, the community thinks, deter potential adversaries from even applying for employment

*Ibid., p. 8.

**Ibid., p. 40. In the second part of the Battelle report, which is addressed in Section 5.3.2.2, Battelle's favored alternative to heavy reliance on clearances is addressed. We also understand that DOE is asking Battelle to examine more closely the currently used criteria for clearances and to develop criteria that would be, in Battelle's judgment, more effective in mitigating insider threats to SNM.

at their agencies. What can be proven empirically is that many applicants withdraw their applications once informed that derogatory information has been developed during their background investigations. Data on AEC security clearances included in the Battelle study support this argument. Of the 12,897 applicants on whom substantially derogatory information was developed between 1947 and 1972, nearly half dropped their request for a clearance.* Thus, clearances appear to deter potentially undesirable candidates from pursuing their applications for employment.

On the other hand, the Battelle study points out that although derogatory information had been developed on over half of the 12,897 applicants, for nearly every applicant (91%) who pursued his request and underwent administrative review, some explanation or qualification of the information was made, resulting in clearance award.**

5.4.2.2 Behavioral Observation Programs

Although quite a few of the government agencies and private industries we contacted incorporate some information on indicators of potential malevolence in their management training programs and expect supervisors to be alert to abnormal behavior in their subordinates, only DOD employs formally structured behavioral observation as part of a security program, the Nuclear Weapon Personnel Reliability Program (PRP).***

*Ibid., p. 15.
**Ibid.
***DOD's Chemical Surety Program PRP is patterned after the nuclear PRP. The Department of Energy's "Personnel Assurance Program (PAP)" charges supervisors with day-to-day observation of employees in critical positions sociated with SNM in terms of their suitability for continued assignment, but the PAP is part of the DOD Nuclear Weapon Safety Program (emphasis added). Although the PAP is a safety program, it has arguable impact on the security area as well.

DOD Directive 5210.42 defines the policy on the nuclear weapons PRP as follows:

> The destructive power of nuclear weapons and the importance of their contribution to our strategic deterrent and tactical capability warrant extraordinary measures to ensure that such weapons are not subject to loss, theft, sabotage, unauthorized use, unauthorized destruction, accidental damage, or jettison. The national security and welfare require, therefore, that only those who have demonstrated unswerving loyalty, integrity, trustworthiness, and discretion of the highest order shall be employed in the nuclear weapon PRP positions.*

The PRP involves both initial screening (security investigation, clearance and medical evaluation) and continuing evaluation of certified individuals' health, attitude, behavior and duty performance. Any of the following traits or conduct are considered grounds for disqualification from the PRP: **

(a) Alcohol abuse

(b) Drug abuse

(c) Negligence or delinquency in performance of duty

(d) Courts-martial or civil convictions that indicate a contemptuous attitude toward the law or other duly constituted authority

(e) Any significant physical, mental or character trait, or aberrant behavior substantiated by competent medical authority that is prejudicial to reliable performance in critical or controlled positions***

(f) Poor attitude or lack of motivation.

---

*U.S. Department of Defense, Nuclear Weapon Personnel Reliability Program (Washington: DOD Directive No. 5210.42, 1978), p. 2.

**Ibid., p. 4.

***A critical position is one that involves access and application of technical knowledge to nuclear weapons; or one whose incumbent can cause the launch or employment of a nuclear weapon or is involved in other phases of weapon control or release (control/use of seals, codes, etc.). A controlled position is one that involves access to or control of access to but no technical knowledge of nuclear weapons; or one whose incumbent is armed and in his security-related duties could inflict damage upon a nuclear weapon or its delivery system.

Although permanent disqualification from the PRP is not punitive and does not necessarily constitute grounds for disciplinary measures, several experts we talked to within DOD and the Department of the Army admit that, on the practical side, a certain, inescapable stigma is associated with PRP decertification.

Table G.25 contains a comparison of disqualification factors for PRP decertifications in 1978. Drug abuse accounts for more disqualifications than any other factor, with the overall disqualification rate equalling 4.99%. Post-certification disqualification tables provided to us by DOD's Office of Security Policy indicate that this overall disqualification rate of about 5% has remained consistent over the last four years. Interviews with representatives of the Army's Military Personnel Center revealed that in 1978, 88% of the Army's PRP disqualifications were among enlisted men from E1-E4, 7% were E5's, 4.5% were E6 and above enlisted men, and .5% were officers or warrant officers.

Although PRP experts admit there are problems with the program, not the least of which is the natural reluctance of members to inform on co-workers,* they point to the lack of nuclear weapons-related insider malevolence as testimony to the program's effectiveness and attribute its success to the combined effects of clearances and behavioral observation.** As one representative of DOD's Office of Security Policy put it, "I don't believe a clearance means a thing unless you invoke supervisory surveillance."

The previously mentioned Battelle study included an evaluation of the U.S. Air Force PRP and DOE's Personnel Assurance Program (PAP). Battelle points out that, like the DOD program, the PAP is based on a "screening-plus-observation" strategy,

*All PRP personnel, not just supervisors and medical personnel, are required to observe and report any incident or condition that may result in temporary or permanent disqualification of a PRP member.
**The Chemical Surety PRP has a similar record of success.

observation accomplished through annual and "as directed" medical evaluations and day-to-day observation. The ability to suspend certification quickly should an unreliability issue surface is an important aspect of both programs.

Battelle's conclusions on the effectiveness of personnel reliability programs in mitigating the insider threat to SNM are the following.*

(a) By emphasizing detection and continuous observation, PRP's avoid many of the difficulties that plague prediction-oriented, constant environment programs (viz., clearances).

(b) Because PRP's focus on work performance both before and after entrance, screening data can be treated as baseline "stable" behavior against which to compare future behavior.

(c) Official enumerations of the criteria or behavior that represent "unreliability" are ambiguous.

(d) Difficulties arise in implementing continuous observation without explicit training for supervisory personnel.

Finally, the study states: "The extent to which a PRP is effective would be considerably enhanced by tightening the definitions of criteria and the procedures for human observation of employee behavior."**

Among the security experts interviewed, many professed their belief that careful, continuous monitoring of employee conduct by supervisors who are trained to be alert to aberrant behavior and emotional changes in their subordinates is an effective means of reducing the insider threat. None demonstrated complete negativism on this issue, although several showed concern about the appropriateness of such a program in the private sector.

*Battelle, pp. 45, 46, 55.
**Ibid., pp. 55, 56.

Two of the consultants to the study capsulized their interviews on this issue by noting respectively that: (1) most industries contacted have an informal system to detect sudden personality changes in employees assigned to sensitive areas; and (2) although screening has some degree of effectiveness in eliminating undesirable applicants, a continuing screening or investigative process is needed to further reduce the probability of crime.* A third consultant offered examples to support his belief that security clearances must be supplemented by strict procedural controls and periodic monitoring of employee conduct if they are to be effective in assuring employee honesty.**

In its analysis of safeguards measures that protect against sabotage of a power plant by two insiders, SAI states:

> Supervisory personnel can also play a useful role in looking for indicators of aberrant behavior of their subordinates. The efficacy of this measure obviously depends on the attentiveness and skill of the plant managers in detecting these indicators.***

The MC&A Task Force report admits that personnel reliability programs "can be used to minimize the possibility of a conspiracy forming effectively...,"**** but questions the practicality and appropriateness of such programs for the civilian nuclear industry because of their use of peer observation and psychological testing.

The University of Minnesota study discussed earlier sheds some indirect light on the subject of behavioral observation. Its research found consistent patterns of counter-productive behavior among some employees (e.g., excessively long lunch and coffee breaks, slow or sloppy workmanship, and phony justification for use of sick leave). Although such conduct can hardly be considered "aberrant

*Brittell, p. 3 and Sutton, p. 3.
**Schechter, p. A6.
***SAI, p. 50.
****MC&A Task Force Report, p. VI-58.

behavior," it may be meaningful that persons who reported above-average theft levels were also quite likely to indicate above-average counter-productive behavior levels. Further, factors that best correlated with theft involvement were also predictive of counter-productive activity. In short, the study says, "...these data suggest that theft may have its roots in the less serious and more prevalent forms of workplace deviance."* Its conclusion that employees who see no negative reaction to the more innocuous forms of employee misbehavior "may conclude that theft of company property will also be tolerated or at least passively ignored"** can be a lesson to any industry, but it also lends credence to the fact that less serious forms of workplace negligence or delinquency can be predictive of insider threats.

5.4.2.3 Psychological Assessment Techniques

Few of the experts we interviewed offered opinions on the value of psychological assessment, but those who did were more often favorably disposed to its use. Because of Privacy Act and civil rights considerations, however, most of the industries we communicated with do not employ psychological profiling during the preemployment process. Some do conduct psychological evaluations of employees assigned to sensitive positions, and a metropolitan police department we contacted gives psychological tests to its officers before allowing them to be armed and put on the street.***

Several intelligence agencies employ psychological testing in the selection process, and the PAP and the nuclear and chemical PRP's incorporate psychological evaluation in the screening phase. One intelligence agency indicated to us

*Theft by Employees in Work Organizations, p. 4.

**Ibid.

***Consultant Brittell, a retired Commander with the Los Angeles Police Department, informed us that most major police department employ this technique. Also, psychologists resident on major police department staffs are available for psychological counseling at the request of an officer or his supervisor.

that most of its 30% screen-out rate results from unfavorable psychological evaluations, while another revealed that poor polygraph results account for the majority of its overall rejection rate of 22%.

As noted in the behavioral observation section, the MC&A Task Force questioned the appropriateness of a PRP-type program explicitly because it involves psychological testing. The SAI study grants the value of periodic post-employment profiling, but counters that "it is not clear what actions can and should be taken in the event that an employee's psychological profile indicates that the employee is unstable."* The authors of the SAI study, who admittedly are not psychologists, fear that indications of instability are "very likely" to occur for persons who would never be capable of or even consider committing an act of sabotage.

This fear is not shared by one of our interviewees, a behavioral scientist with approximately ten years of law enforcement and intelligence experience. He argues that the art of psychological assessment has advanced to the degree that professional assessors (and he emphasizes professionalism) can make very accurate personality evaluations that can determine stress, its degree and cause, and the subject's weaknesses and strengths. This source, whose expertise lies primarily in the field of terrorism, recommends that the nuclear industry adopt a psychological profiling program for selection and monitoring of key personnel, that supervisory personnel be trained to recognize warning indicators and even administer the tests, but that trained professionals be used for the assessment of test results. Although this source acknowledges the civil and constitutional difficulties that may arise in administering a psychological profile program,

*SAI, p. 49.

he believes that the question of nuclear security is too critical to leave this option unexplored. Finally, he recommends that, should such a program be adopted, a concerted effort should be made to sell it to employees in a positive manner.

5.4.2.4 Management-Employee, Management-Security and Security-Employee Rapport

Without exception, development of a healthy relationship between management and employees was considered a crucial aspect of good security. Consultant Brittell summarized the feeling of his interviewees on this issue as follows:

> ...the best control of the insider threat is by directing the security effort towards proper personnel management, not by electronic or mechanical means. Professional personnel selection, training, motivation, supervision, ethics and the development of a sound employee relations program are paramount to reducing employee misconduct.*

The results of the University of Minnesota study add credence to this belief:

> ...the dissatisfied employee was found to be more frequently involved in employee theft.**
>
> The most consistent sources of dissatisfaction seemed to be the supervisor and the employer. Where the supervisory personnel were viewed as unhelpful, incompetent and unconcerned, higher theft was detected. Where the integrity, fairness and ethical quality of the company were questioned, more theft was found.***

The following suggestions for improving management/employee relations represent the opinions of both our interviewees and our consultants:

(1) Solicit Employee Suggestions on the Best Way to Implement Rules and Regulations

Employees are less likely to resent procedures they have had a share in formulating. The most efficient ideas for implementing a regulation often come from someone directly involved at the point of action.

*Brittell, p. 1.
**Theft by Employees in Work Organizations, p. 4.
***Ibid., p. 5.

(2) Provide a Grievance Committee for Evaluation of Worker Complaints

This may serve as an outlet for at least some of the frustration that a disgruntled employee might otherwise channel into subversive activities.

(3) Provide Recognition for Employee Performance

Employees whose performance and loyalty go unrecognized or unappreciated tend to become, at best, dissatisfied and, at worst, disgruntled. A little positive reinforcement can go a long way at all levels and is especially important for employees in routine, low-profile jobs.

(4) Offer Workshops in Participative Management

In direct contrast to authoritarian management, this form of management tends to reduce frustration by directly involving workers in the decision-making, problem-solving and goal-setting processes related to their own jobs.

(5) Encourage a Team Approach to Operations

The team approach is considered an excellent means for building employee morale and for engendering a sense of proprietorship, which is extremely beneficial to security. When this approach is taken, employees are more likely to report illicit activities, which are a threat to their team, and alienated workers will stand out readily from the others.

(6) Provide Free Psychological Services to Employees

Emotional difficulties arising not only from a person's job but from his private life can sometimes build up until the employee reacts in an anti-social manner, in some cases by malevolent behavior. A number of firms and agencies have assigned to their personnel departments trained professional counselors whose full-time job is to provide confidential assistance to employees with private or job-related problems.

(7) Require That All Employees Be Subject to the Same Security Procedures

To show varying degrees of trust in personnel on the basis of rank will lead to considerable ill-will by implying that employees at the bottom rung in particular are not to be trusted.

Clearly, good management-employee rapport does not develop automatically; it must be intelligently and aggressively pursued by management.

Equally important to safeguards effectiveness is the establishment of a good rapport between management and security. A security organization that is treated as a non-profitmaking but necessary evil by management is likely to be a weak one because this corporate attitude inevitably permeates the rank and file. To be effective, the director of security must have direct access to the company's chief administrative officer, and the security force should be independent of operational management.

Several of our interviewees commented that some federal inspectors have helped create a poor security image in the eyes of corporate management. These inspectors, lacking in tact and sometimes in technical knowledge, have lectured high-ranking corporate officers in "school boy" fashion for minor security infractions. In the process, they have downgraded the image of the security department. In addition, their frequent use of the terms "guard" and "guard force" instead of "security officer" and " security force" tends to reinforce corporate biases against security. A more tactful, positive attitude on the part of such inspectors can reduce such biases.

Finally, general agreement was voiced on the need to foster employee respect for and acceptance of security. First and foremost should be a thorough program of security education for all employees. Although the effectiveness of security education is often sneered at by cynics (usually employees), a well-administered

program can contribute greatly to overcoming employee resentment of regulations, increasing resistance to corruption, and integrating employees into the security monitoring process. Use of case histories and examples of how employees "just like you" have been compromised by both insiders and outsiders are particularly helpful in creating an interesting and meaningful program.

Unique security-consciousness techniques were used by two of the companies we contacted. The first company radically changed the image of its security force after one of its employees had been involved in a major espionage case. As part of the new approach, it sponsored professional security seminars for all its employees. Speakers from the FBI, CIA and NSA were used. The subject matter was understandable, practical and believable. Each seminar was opened by a senior company vice-president to demonstrate management's support for the security program.

The second company held a "security fair" which employees attended on company time. The fair had a personal, practical theme: employees were told how to protect themselves and their property by means of instructions about the capabilities and limitations of smoke alarms, locks, burglar alarms and other security devices. Selected vendors displayed their products and sold them at wholesale prices to employees. At the same time, a pitch was made about the company's security program. The company's security staff also holds annual one-on-one interviews with employees assigned to sensitive positions.

5.4.2.5 Other Prevention Strategies

The four preceding sections dealt with measures that may reduce the probability of an attempt at theft or sabotage. This section addresses measures aimed at reducing the probability of success given that an attempt is made.

Security experts suggested a number of such measures, some of which are already used to some degree by the nuclear industry at large. The following techniques were recommended most often by our interviewees. In some cases, their recommendations were qualified as indicated.

(1) Dual Custody of Sensitive Material

Although dual custody was generally recommended, several experts noted that, if allowed to continue without rotation, its effectiveness can be degraded since it may lead to too high a degree of familiarity between the persons sharing custody.

(2) Division of Responsibility

This fundamental principle of security can make the goals of a single adversary quite difficult to fulfill. Restricting the duties and authority of individuals limits the extent to which authority can be abused by any one person. The keys to this measure's effectiveness are intelligent application and a strong policy of enforcement.

(3) Rotation of Duties

In Safeguards against Insider Collusion, a study done for NRC by Science Applications, Inc., SAI states that in defining an appropriate span for rotating job assignments (both security officers and operational personnel), two actions may be taken to reduce the risk of partial theft sequences being successful. These are a "search or facility sweep for hidden material and/or a physical inventory of material prior to job rotation."*

*T. L. McDaniel et al., Safeguards against Insider Collusion (Washington: U.S. Nuclear Regulatory Commission, NUREG/CR-0532, vol. 1, prepared under contract by Science Applications, Inc., 1979), p. 6.

(4) Compartmentalization

The same SAI study addresses compartmentalization in its analysis of area zoning and function zoning--restricting where people can work and what tasks they can do. SAI finds area zoning to be especially useful for nuclear facilities when the safeguards system consists of concentric zones surrounding the material assess area or vital area so that a number of control zones (no matter how diverse their safeguards) must be crossed by an adversary to reach his target and exit. Function zoning applies well when the safeguards system consists of a single zone or barrier with many different types of safeguards in the zone or at the barrier. SAI admits that these two types of work rules may reduce safeguards vigilance because they restrict an employee to one function or to a single location. They suggest instituting carefully scheduled rotation to ameliorate this condition.

(5) Security Audits

Unannounced and independent inspections of the security system, tactics simulations, sensor testing, and test stimuli for security officers were all given high marks as means of heightening the alert posture of a security force.

(6) CCTV

Almost without exception, security experts recommended use of CCTV. Several consider CCTV a more effective preventive measure when it is associated with motion detectors and audio capability.

APPENDIX A

LIST OF ACKNOWLEDGMENTS

We offer our appreciation to the following people who contributed their advice, guidance, and opinions during the course of the study:

Mr. Arthur D. Burger
Attorney at Law
Washington, DC

Ms. Teuta Cohen
Psychologist
New York, NY

Mr. E.J. Criscuoli, Jr.
Executive Director
American Society for
Industrial Security
Washington, DC

Mr. William B. Cummings
Former U.S. Attorney
Eastern District of Virginia
Alexandria, VA
(currently in private practice)

Mr. John Graziano
Assistant Inspector General
for Investigations
U.S. Department of Commerce
Washington, DC

Mr. Karl Koch
Director of Training
Department of Economic Community
Development
Division of Crime Prevention
Columbus, OH

Mr. Philip R. Manuel
Former Chief Investigator
U.S. Senate Subcommittee on
Permanent Investigations
Washington, DC
(currently a private consultant)

Mr. David J. Ontell
Attorney at Law
Washington, DC

Mr. William F. Reed
Attorney at Law
Washington, DC

Mr. Richard Ross
Attorney at Law
Washington, DC

Mr. Lewis C. Schneider
Manager, Education and Seminar
Division
American Society for Industrial
Security
Washington, DC

Mr. Justin Williams
U.S. Attorney
Eastern District of Virginia
Alexandria, VA

Dade County, Florida Public
Safety Department:
- Capt. John A. Beckman
- Mr. Paul H. Bohardt
- Mr. William H. Dunman
(Institute on Organized
Crime)
- Mr. Bruce H. Jones
(Institute on Organized
Crime)
- Mr. Carl D. Van Atter

APPENDIX B

LAWRENCE LIVERMORE LABORATORY RESEARCH

1. INTRODUCTION

The Lawrence Livermore Laboratory (LLL) research project (RES 79-11) was primarily subcontracted to J. M. Heineke and Associates. Dr. Heineke, a professor of economics at the University of Santa Clara, is a leading expert in adversary modeling. His report, "The Insider Threat to Security Facilities: Data Analysis," NUREG-1234 (to be published in June 1980), provides statistical analyses and interpretation of three data sets derived from analogous industries and activities: bank fraud and embezzlement (BF&E), computer crime in a number of industries that are directly dependent on electronic computing for accounting and inventory control, and drug thefts. Mr. Richard Schechter of LLL served as project coordinator and, indeed, collaborated with Dr. Heineke throughout most phases of the research. The results of their efforts are summarized below.

2. METHODOLOGY AND LIMITATIONS

The LLL data were subjected to analysis using both formal statistical techniques (linear regression equations) and descriptive techniques (displaying empirical relationships between variables in a series of tables). The BF&E and computer crime data sets were large (313 and 461 respectively) and contain information on a case basis. Because the drug data were available only as aggregates, no detail on individual thefts could be derived. Consequently, LLL was unable to provide the same level of statistical and interpretative detail on drug thefts as they provided for the other two data sets.

3. BANK FRAUD AND EMBEZZLEMENT

3.2 Data Description

The bank fraud and embezzlement data set was made available to LLL by the Intelligence Section of the Federal Deposit Insurance Corporation (FDIC) and is comprised of 313 bank defalcation cases with losses or potential losses* of $10,000 or more reported to FDIC in 1976 and 1977. Variables examined are: perpetrator position (target control), group size, bond coverage per incident, method of detection, concealment time, loss size, and bank size.** The data set contains information on suspects, not on convicted perpetrators.

3.2 Analysis

3.2.1 Position (Target Control)

Observations related to the position of the highest ranking perpetrator are as follow:

(1) Predicted losses are by far the highest when the highest ranking perpetrator is an executive (bank president or director) (Table B.1). It appears that the relatively greater account accessibility of bank presidents and directors and the relative autonomy of their actions lead to higher expected gains from BF&E than for any other group of employees.

(2) Differences in potential losses as bank size changes are significant if the perpetrator is an executive, but not as dramatic as for the staff perpetrator (non-management employee) (Table B-1).

---

*The amount of money involved in an incident may properly be termed the "potential loss" since, in some instances, a portion of this amount is recovered.

**Rankings are assigned to banks by the American Banking Association (ABA) as a function of their deposits; rankings range from Group 1 (less than $750,000 in deposits) to Group 20 (more than $2 billion in deposits).

Table B.1

Predicted Losses, Perpetrator Position and Bank Size*

Predicted (Potential) Loss Size ($1000)	Highest Ranking Perpetrator	Bank Size** (ABA No. in paren.)
145.14	EXEC	small (5)
96.24	MGT***	small (5)
3.50	STAFF	small (5)
203.25	EXEC	average (11)
154.08	MGT***	average (11)
61.34	STAFF	average (11)
280.37	EXEC	large (19)
231.20	MGT***	large (19)
138.40	STAFF	large (19)

* Losses are calculated for the case in which the number of perpetrators is one and when employee bond coverage = $1,400 (the sample mean).

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

*** Since the data for top management and low/middle management were not statistically different, we use MGT to represent all management.

3.2.2 Group Size and Conspiracy

The following observations were made from Tables B.2 through B.6:

(1) Executives are far more likely to be involved in conspiracy than employees at any other level (Table B.2). A full 71% of the cases involving executives involved more than one perpetrator. This seems to stem from the fact that executives are in a unique position to encourage cooperation from underlings. In addition, a bank president, unlike 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 accessibility is needed to carry out a crime.

(2) The average size of the conspiracy is larger when executives are involved (Table B.3).

(3) The lone insider accounts for 61% of the 274 cases in which the number of perpetrators was known (Table B.4).

(4) Insiders in conspiracy with other insiders and with outsiders account for 18% and 21% respectively of the 296 cases in which this information was available (Table B.5).

(5) Conspiracy size has a substantial impact on potential BF&E losses (Table B.6). For an average size bank ($25-35 million in deposits), predicted losses increase from $203 million to $238 million per incident by going from one adversary to a small, two-person conspiracy.

3.2.3 Bond Coverage

The bond coverage variable is a measure of total bond coverage per incident for an entire bank, including branch offices. Table B.7 reveals that the higher the bond coverage, the lower the predicted loss size. LLL hypothesizes that the

Table B.2

Distribution of Collusive Attacks on Banks, Conditional on Perpetrator Position: BF&E Cases, 1976-77*

given POSITION OF PERPETRATOR** is	Proportion of Cases with Collusion Among Perpetrators				
	Executive	Top Management	Low/Middle Management	Staff	Branch Manager
	.71	.18	.30	.14	.28

* Total number of cases with data on each variable is 286.

** First four positions are mutually exclusive and exhaustive and, in conspiracy cases, list the position of the highest ranking perpetrator. The category branch manager stands alone and is reported whether or not he is the highest ranking perpetrator.

Table B.3

Distribution of Conspiracy Size, Conditional on Position of Perpetrator: BF&E Cases, 1976-77*

		Number of Perpetrators				
		1	2	3	4	5 or greater
given that POSITION** is	Executive	.29	.38	.15	.07	.11
	Top Management	.82	.06	.09	0	.03
	Low/Middle Management	.70	.16	.09	.04	.01
	Staff	.86	.09	.02	0	.03
	Branch Manager	.7	.05	.15	.1	0

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

** Same as ** in Table B.2.

Table B.4

Distribution of Group Size: BF&E Cases, 1976-77*

Number of Perpetrators				
1	2	3	4	5 or greater
.61	.21	.10	.03	.04

* Total number of cases used in table is 274.

Table B.5

Distribution of Perpetrators by Type of Group:
BF&E Cases, 1976-77*

Single Perpetrator	Insider with Other Insider(s)	Insider with Outsider(s)
.61	.18	.21

* Total number of cases is 296.

Table B.6

Predicted Losses, the Number of Perpetrators and Bank Size

Predicted (Potential) Loss Size* ($1000)	Number of Perpetrators	Bank Size**
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)

* Losses are calculated for case when highest ranking perpetrator is an executive and BOND = $1,400, the sample mean.

** See footnote ** after Table B.1.

amount of employee bond coverage is an indicator of management's awareness of the insider threat and of the attention given by management to internal controls. Such awareness of the general BF&E problem, in turn, results in higher bonds, tighter controls and, as shown in Table B.7, lower loss size per incident.

Table B.7

Predicted Losses, Employee Bond Coverage and Bank Size

Predicted (Potential) Loss Size* ($1000)	Bond Coverage ($1000)	Bank Size
121.01	Low ($125)	Small (5)
102.01	Mean ($1400)	Small (5)
43.01	High ($5000)	Small (5)
178.85	Low ($125)	Average (11)
159.85	Mean ($1400)	Average (11)
100.85	High ($5000)	Average (11)
255.97	Low ($125)	Large (19)
236.97	Mean ($1400)	Large (19)
177.97	High ($5000)	Large (19)

* Losses are calculated for cases when there is one perpetrator who is an executive.

3.2.4 Method of Detection

Tables B.8, B.9 and B.10 yield the following observations:

(1) Executives and top management (senior vice-presidents, treasurers, trust officers) are more likely to be caught by means of bank examinations than internal audits, whereas low/middle management and staff are much more likely to be detected in an internal audit (Table B.8). This observation dramatically

accents the lack of independence between internal auditors and the top officials of a bank--a fact emphasized by federal bank examiners interviewed. In the case of branch managers, audits are done by the parent bank, which has all the proper incentives for uncovering a defalcation.

(2) Confessions are most likely from lowest level perpetrators and least likely from higher-level perpetrators (Table 8.8).

(3) Outsiders are most likely to aid in the detection of staffers and least likely to aid in the detection of a bank president (Table 8.8). This is no doubt due to the fact that the amount of interaction with the public decreases with position.

(4) External bank examinations are not an effective method of detection when large (five or more) conspiracies are operating (Table 8.9). This presumably reflects the fact that large groups working together can usually disguise manipulations, at least during the rather short visits of examiners.

(5) Confession is the likeliest method of detection of large conspiracies (Table 8.9). This demonstrates the obvious "Achilles heel" of large conspiracies: as group size grows, it becomes increasingly likely that an individual will become involved with the group who has less stability to withstand the tension associated with endless accounting coverups. Confessions in large conspiracies are approximately twice as likely as in any other group.

(6) Overall, bank examinations, internal audits and confessions are equally representative methods of detection (Table 8.10).

Table B.8

Distribution of Method of Detection, Conditional on Position of Perpetrator: BF&E Cases, 1976-77*

		METHOD OF DETECTION***					
		Bank Examination	Audit	Insider Information	Outsider Information	Confession	Absence
given that POSITION** is	Executive	.41	.20	.06	.11	.20	.01
	Top Management	.29	.23	.10	.13	.23	.03
	Low/Middle Management	.12	.32	.05	.17	.33	.01
	Staff	.10	.29	0	.19	.40	.02
	Branch Manager	.11	.42	.11	.11	.26	0

* Total number of cases with data on each variables is 272. Rounding error may cause totals to deviate slightly from one.

** First four positions are usually exclusive and exhaustive and, in conspiracy cases, list the position of the highest ranking perpetrator. The category "Branch Manager" stands alone and is reported whether or not Branch Manager is the highest ranking perpetrator.

*** The following definitions were used:
(a) "Bank examination" represents a state or federal examination.
(b) "Audit" usually represents an internal audit, but occasionally indicates audit by outside firm.
(c) "Insider information" indicates perpetrator was detected via information furnished by fellow employee.
(d) "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.
(e) "Confession" indicates both out and out confessions and errors on the part of perpetrator which lead to confession.
(f) "Absence" indicates perpetrator was detected while absent--usually on vacation or after death.

Table B.9

Distribution of Method of Detection, Conditional on Number of Perpetrators: BF&E Cases, 1976-77*

		Method of Detection**					
		Bank Examination	Audit	Insider Information	Outsider Information	Confession	Absence
given that NUMBER OF PERPETRATORS is	1	.17	.30	.05	.18	.29	.01
	2	.24	.28	.05	.1	.29	.03
	3	.37	.19	.07	.15	.22	0
	4	.45	.09	.09	.09	.27	0
	5 or greater	.15	.31	0	.08	.46	0

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

** For definitions, see Table B.8.

Table B.10

Frequency of Detection by Method: BF&E Cases, 1977-77*

Bank Examination	Audit	Insider Information	Outsider Information	Confession	Absence
.25	.26	.05	.14	.28	.01

* Total number of cases with data on method of detection is 295.

3.2.5 Concealment Time

Table B.11 reveals that, on the average, executives are not able to conceal BF&E's as long as other managers. According to LLL, the only explanation for this apparent anomaly lies in the thoroughness of auditing procedures as a function of the position of the individuals responsible for the transactions or accounts: federal examiners often examine the transactions of executives 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.

Table B.11

Distribution of Time Concealed, Conditional on Perpetrator Position: BF&E Cases, 1976-77*

		Time Concealed***		
		Short	Medium	Long
given that POSITION** is	Executive	.21	.60	.19
	Top Management	.43	.29	.29
	Low/Middle Management	.34	.37	.29
	Staff	.66	.24	.1
	Branch Manager	.5	.3	.2

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

** First four positions are mutually exclusive and exhaustive and, in conspiracy cases, list the position of the highest ranking perpetrator. The category "Branch Manager" stands alone and is reported whether or not Branch Manager is the highest ranking perpetrator.

*** 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

3.2.6 Probability of Branch Manager Involvement in BF&E

Since branch managers appear to offer the closest analog to the plant manager in a nuclear facility, LLL computed an estimate of the probability that a branch manager will attempt a BF&E. This probability was estimated by using the ratio of the total number of branch managers in FDIC-regulated banks involved in a BF&E in 1976-1977 divided by the total number of branches in FDIC-regulated banks in that period. That ratio is .0020, indicating that over the 1976-1977 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. Since a few "branches" will in fact be automated teller machines, our data indicate that more than two of every thousand managers are engaged in embezzlement.

3.3 Conclusions

LLL's study draws the following conclusions with respect to the analog between BF&E and potential nuclear malevolence:

(1) The negative impact of bond coverage on loss size indicates that indirect methods of generating a secure environment may be useful to regulators in checking for adherence to regulatory codes. If a variable can be identified that is highly correlated with a desired activity (as is employee bond coverage with tight internal controls), then observing the deviation of this variable from the industry mean would provide an indirect check on the level of the desired activity.

(2) Interviews with FDIC investigators reveal that high acquittal rates for BF&E and the concomitant fear on the part of bankers that a libel suit will be riled result in bankers often finding it safer to take the loss and learn from the experience. LLL feels that this point should be a fundamental consideration for authorities charged with securing nuclear facilities. Namely, every possible effort must be made to insure conviction of guilty adversaries and not to be complacent with the knowledge that "we got him." Low conviction rates have very undesirable incentive effects.

(3) The clear lack of independence between internal auditors and top bank officals (as revealed in Section 3.2.4(1) above) offers a strong analog to the nuclear industry. Great care must be taken to insure that industry security managers and inspectors are truly independent in the sense that their position or livelihood could in no way be affected by an adverse report concerning plant operations.

In a separate report, Mr. Richard Schechter of LLL reported the results of his interviews with members of FDIC's Intelligence Division and his review of BF&E case histories. The more pertinent of his opinions and observations are:

(1) Conspiracy Formation

FDIC experts believe that BF&E conspiracies usually begin with one employee being asked to make a seemingly innocent departure from formal procedures for the convenience of a co-worker whom he does not suspect of dishonesty. By the time he discovers that his co-worker is actually involved in illicit activities, he, too, has been implicated and is compelled to take part in the subsequent coverup to protect his own job.

(2) Modus Operandi

Many of the BF&E cases involved a modus operandi that appears somewhat analogous to potential threats in the nuclear industry: false entries into ledgers, as well as alteration, destruction and forgery of records. These findings reflect the importance of maintaining multiple sets of well-separated records, which are occasionally checked against each other as well as against actual inventories. Also, the prominence of signature forgery in BF&E would support the use of automated signature verification.

Another common modus operandi was the issuance of unauthorized loans; bank employees will often exceed their official authority limits if there is no actual mechanism to prevent this. Fictitious loans recorded as having been

made to previous bank customers were also typical. This illustrates the importance of immediately verifying all shipments of nuclear material independently of the person who recorded the transaction.

(3) Operational Deficiencies

A large proportion of cases cited a system that enabled a single person to perform all of the steps necessary for an embezzlement. Such deficiencies were expressed with the captions "one-man operation of bank," "ill-defined authority limits," and "failure to separate and rotate duties." A well-designed security system must rigorously define the limits of each person's authority and separate individual duties so that a specified minimum number of persons would be required to complete a diversion. Should rotation of duties among workers with similar functions be feasible, it would severely complicate the formation of conspiracies, especially if assignments were made with a randomized schedule.

Another ailment in banking security is that many institutions appear to be run as "family type operations," in which banking officers are granted an inordinate level of trust by virtue of their position.

One way in which the nuclear industry might help to reduce the difficulties mentioned above would be through an intensive security education program for all personnel. Such a program might provide each employee: (a) instructions on just what authority limits exist for himself and his co-workers and exactly what his supervisor can and cannot order him to do; (b) information on how to detect a suspicious irregularity in standard procedures and what to do when he has discovered something suspicious; and (c) an awareness of the need for security through a discussion of insider theft in analogous situations, as well as a discussion of the possible consequences of a successful diversion.

"Dual controls," the banking industry's version of the "two-man rule," are often circumvented in BF&E incidents due to lack of effective enforcement. This fact is of grave concern to the nuclear industry where, in many cases, the implementation of the two-man rule depends on the "honor system," with no means of verification other than dual signatures, which can easily be forged. Mr. Schechter recommends that wherever possible, automated procedures be established to require the physical presence of two authorized persons for especially sensitive operations. In addition, a strong position should be taken by management that a person who signs his name to the completion of a two-man operation will be held responsible for any irregularities that transpired, even if he was simply negligent in overlooking a mistake by his partner. Such a policy might go a long way toward countering the deleterious effect on security of familiarity among workers.

(4) Method of Detection

BF&E perpetrators seem to benefit from a reluctance of fellow workers to disclose their irregularities to management or the Board of Directors. In cases where an informant was responsible for a disclosure, it was usually performed anonymously. If anonymity is indeed a facilitating factor for disclosure of potential indiscretions, then security systems should be designed to exploit this fact.

The detection data also reveal a surprisingly high number of incidents that came to light during the absence of a suspect, due to either vacation, illness, resignation, death, or dismissal for reasons unrelated to the case. Indeed, many BF&E schemes require continuous doctoring of the records over an indefinite time period. Thus, a mandatory, continuous

two-week vacation period is considered an effective security meansure in the banking industry. For this tack to be fully effective, an employee should be prevented from entering the facility for any reason whatsoever during his vacation. This technique might be readily implemented in the nuclear industry.

4. COMPUTER CRIME

4.1 Data Description

The data in this section were made available to LLL by Donn Parker of Stanford Research Institute International in Palo Alto, California.* The data set contains 461 incidents (1958-1978) and includes information on position of the perpetrator, group size, crime type, victim type, loss size and the disposition of individual cases. It should be noted that the data base includes a variety of crime types (theft and sabotage among them), 41 cases in which no insider was involved, and 13 in which a former employee was involved.

4.2 Analysis

4.2.1 Position (Target Control)

The following observations are derived from Tables B.12 and B.13:

(1) When a lone executive is the perpetrator, losses are over nine times larger than those suffered when any other insider acting alone is the perpetrator. In fact, losses are systematically higher when an executive is involved, no matter how many individuals are colluding (Table B.12).

(2) Given that the number of perpetrators is four or more, executives are more likely to be involved in a computer crime than any other type of employee (Table B.13). Table B.12 shows that collusion pays off, and since executives

*Mr. Parker is the author of Crime by Computer (New York: Charles Scribner's Sons, 1976).

have more authority and less direct operational control than other personnel within a firm, it should be both easier and more necessary for them to form conspiracies.

Table B.12

Predicted Losses and the Number and Type of Perpetrator: Computer Crimes

Predicted Loss ($1000)* per Incident	Number of Perpetrators**	Type of Perpetrator
1478.18	1	Executive
1734.19	2.5	Executive
2160.90	5	Executive
3014.30	10	Executive
158.51	1	All Others***
414.53	2.5(mean)	All Others
841.23	5	All Others
1694.63	10	All Others

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

** The number of perpetrators varies between 1 and 60 in the sample.

*** "All others" indicates that highest ranking perpetrator(s) is/are individual(s) below executive in rank and includes cases in which the perpetrator is unknown but excluded cases in which a corporation is the perpetrator. Corporate perpetrators were excluded because a few very large losses inflicted by them are far above the mean loss and tend to skew the data if included.

Table B.13

Distribution of Perpetrator Position, Conditional on Number of Perpetrators: Computer Crimes, 1958-78*

		Perpetrator Position**								
		Exec.	Cemp	Ncemp	Unemp	Corp	Outsider	Student	Exemp	Unknown
given Number of PERPE-TRATORS is	1	.15	.22	.16	.21	0	.09	.07	.05	.06
	2	.15	.22	.25	.17	.02	.07	.1	.03	0
	3	.18	.32	.14	.05	.05	.09	.18	0	0
	4	.38	.23	.23	0	0	.08	.08	0	0
	5 or greater	.16	.08	.19	.35	.05	.05	.11	0	0

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

** The following abbreviations were used (in conspiracies, position of the highest ranking perpetrator was used):

EXEC: executive
CEMP: computer employee
NCEMP: noncomputer employee
UNEMP: unknown employee
CORP: corporation (a corporation, often a competitor, is the perpetrator)
EXEMP: ex-employee

4.2.2 Group Size and Conspiracy

(1) When only insiders are involved, expected losses are consistently higher than when an outsider is involved (acting alone, with other outsiders, or with insiders) (Table B.14).

(2) Sixty-four percent of all cases involved a single adversary, but perpetrators in collusion account for over one-third of the available data (380 cases) (Table B.15).

Table B.14

Predicted Losses, Outsider Involvement, Number and Type of Perpetrator: Computer Crimes

Predicted Loss ($1000)*	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 Others**
9203.33	NO	NO (Number of perp =1)	All Others
8307.78	YES	YES (Number of perp =mean)	All Others
9459.35	NO	YES (Number of perp =mean)	All Others
8734.48	YES	YES (Number of perp =5)	All Other
9203.33	NO	YES (Number of perp =5)	All Others

* Losses are calculated for case when victim is financial institution.

** "All others" indicates highest ranking perpetrator(s) is/are individual(s) below the rank of executive and includes cases in which perpetrator is unknown.

Table 8.15

Distribution of Number of Perpetrators:
Computer Crimes, 1958-77*

Number of Perpetrators				
1	2	3	4	5 or greater
.64	.16	.06	.03	.11

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

(3) Within the entire data base, the breakdown of insiders vs. outsiders, by percent, is:

Insiders Alone	55.8
Insider/Outsider Conspiracy	17.3
Insider/Insider Conspiracy	14.3
Outsider Alone or in Conspiracy with Other Outsider(s)	12.4

Thus, although the single insider is the most frequent perpetrator, insiders in conspiracy (31.6%) represent a common and serious threat.

4.2.3 Crime Type (Perpetrator Objective)

(1) The overwhelming objective of most perpetrators is fraud (53.8%); outright theft accounts for 19.6% (information, inventory, hardware and software); sabotage (physical destruction and data destruction) accounts for 13.1% (Table 8.16).

(2) For sabotage (rows 1 and 4 of Table 8.17), single adversaries account for an average of 77% of the cases; for theft (rows 2, 3 and 5), they account for 59%.

(3) Insiders are most likely to collude with outsiders in the perpetration of fraud and inventory theft and least likely to collude with insiders in physical destruction, data destruction and theft of hardware and software (Table 8.18).

Table B.16

Distribution of Type of Crime:
Computer Crimes, 1958-77*

Crime Category	
Physical Destruction (PHYDIST)	.086
Theft of Information (TINFO)	.117
Theft of Inventory (TINV)	.021
Data Destruction (DATADEST)	.045
Theft of Hardware or Software (THW/SW)	.058
Unauthorized Use (NUSE)	.117
Fraud	.538
Error**	.018

* 461 incidents were available for these calculations.

** "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.

4.2.4 Victim Type

(1) No matter what the level of the highest ranking perpetrator, the predicted losses from computer crime are highest for computer service companies and transportation and utility companies respectively and lowest for communications and publication firms and financial institutions (Table B.19).

(2) Transportation and utility companies and sales and manufacturing firms were more often victims of fraud than of any other types of computer crime (Table B.20) and were considerably more likely to be hit by insiders than by outsiders or by insider/outsider conspiracies (Table B.21).

Table B.17

Distribution of Number of Perpetrators, Conditional on Crime Category: Computer Crimes, 1958-78*

		Number of Perpetrators				
		1	2	3	4	5 or greater
given CRIME CATEGORY is**	Phydest	.65	.08	.08	.08	.12
	Tinfo	.58	.23	.05	.05	.09
	Tinv	.25	0	.13	.38	.25
	Datadest	.89	0	.05	0	.05
	Thw/sw	.76	.1	.05	0	.1
	Nuse	.61	.24	.11	0	.04
	Fraud	.64	.17	.05	.03	.12
	Error	.75	0	.25	0	0

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

** For expansion of acronyms, see Table B.16.

Table B.18

Distribution of Perpetrator Location, Conditional on Crime Category: Computer Crimes 1958-78*

		Perpetrator Location		
		Insider	Outsider	Insider/Outsider
given CRIME CATEGORY is	Phydest	.79	.17	.03
	Tinfo	.84	.1	.06
	Tinv	.56	0	.44
	Datadest	.95	.05	0
	Thw/sw	.83	.17	0
	Nuse	.81	.13	.06
	Fraud	.66	.12	.22
	Error	.86	.14	0

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

Table B.19

Predicted Losses, Victim Institution and Type of Perpetrator: Computer Crimes

Predicted Loss ($1000)*	Victim Institution	Type of Perpetrator**
2623.28	Finance	Executive
2797.87	Government	Executive
2899.48	Medical	Executive
3080.40	Educational	Executive
2723.72	Sales & Manufacturing	Executive
1210.79	Communications & Publications	Executive
3263.34	Transportation & Utilities	Executive
5297.99	Computer Service Co.	Executive
1303.61	Finance	All Others
1478.18	Government	All Others
1579.81	Medical	All Others
1760.73	Educational	All Others
1404.05	Sales & Manufacturing	All Others
0***	Communications & Publications	All Others
1943.67	Transportation & Utilities	
3978.32	Computer Service Co.	All Others

* Losses are calculated for case where the number of perpetrators equal one.

** "Executive" is highest ranking perpetrator. Category "all others" signifies highest ranking perpetrator(s) is/are individual(s) below rank of executive and includes cases in which perpetrator is unknown.

*** Predicted loss here is slightly negative but statistically not different from zero.

Table 8.20

Distribution of Crime Category, Conditional on Victimized Institution: Computer Crimes, 1958-78*

		Crime Category							
		Phydest	Tinfo	Tinv	Datadest	Thw/sw	Nuse	Fraud	Error
given VICTIMIZED INSTITUTION** is	Fin	.04	.01	0	.02	.01	0	.93	0
	Govt	.03	.18	.04	.03	.03	.11	.58	.01
	Med	.33	0	0	0	0	0	.67	0
	Educ	.34	.13	0	.02	.09	.3	.11	.02
	Salmfc	.04	.07	.07	.13	.16	.09	.44	0
	Compub	0	.33	0	0	.17	0	.33	.17
	Transutil	.17	0	.17	0	0	0	.67	0
	Compserv	.05	.26	0	0	.14	.24	.31	0
	Proforg	.2	.2	0	.2	0	0	.4	0
	Ind	0	.11	0	0	0	.28	.44	.17

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

** See Table 8.19 for expansion of abbreviations. "Proforg" is a professional organization; "Ind" is an individual.

4.2.5. Probability of Success/Disposition

Probability of success, conditional on some factor x, was estimated by dividing the number of cases characterized by factor x in which the perpetrator was not apprehended by the total number with characteristic x on which case disposition information was available. Table 8.22 contains these estimates for 16 selected variables and reveals the following:

(1) Conspiracies have a 20% higher failure rate than do incidents involving single perpetrators.

(2) Sabotage (physical destruction and data destruction) is likely to succeed 22 times out of 100. This tends to support the conclusion that sabotage is relatively more difficult to trace than other types of computer crime, although the number of data points available for some of these computations is quite small.

Table B.21

Distribution of Perpetrator Location, Conditional on Victimized Institution: Computer Crimes, 1958-78*

		Perpetrator(s) Location		
		Insider(s)	Outsider(s)	Insider/Outsider
given VICTIMIZED INSTITUTION is**	Fin	.61	.19	.21
	Govt	.67	.1	.23
	Med	1.0	0	0
	Educ	.9	.08	.03
	Salmfc	.83	.06	.11
	Compub	.75	.25	0
	Transutil	.67	0	.33
	Compserv	.66	.15	.2
	Proforg	.6	0	.4
	Ind	.88	.06	.06

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

** For expansion of abbreviations, see Table B. 19.

(3) Given that the victimized institution is a transportation or utility company, the probability of success is 14 out of 100. (N.B. Only seven data points were available for this computation.)

4.3 Conclusions

LLL's study draws the following conclusions on the analogy between computer crime and nuclear crime:

(1) 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 a credible threat to the nuclear industry. A number of computer crimes outside the nuclear industry have immediate relevance to potential threats to the nuclear industry. Among them are:

Table B.22

Estimated Probabilities of Success: Computer Crimes

Estimated Probabilities	Crime Type	Size of Subsample Used in Calculation
.115	Single Perpetrator	156
.092	Conspiracy	141
.022	EXEC* Involved	45
.125	CEMP Involved	56
.074	NCEMP Involved	54
.083	EXEMP Involved	12
.304	PHYDEST Crime	23
.200	TINV Crime	5
.182	TINFO Crime	33
.111	DATADEST Crime	9
.105	FRAUD Crime	181
.098	FIN Victim	92
.176	GOVT Victim	51
.143	TRANUTIL Victim	7
.064	COMPSERV Victim	31
.132	SALMFC Victim	38

*The following definitions were used:

EXEC - executive
CEMP - computer employee
NCEMP - non-computer employee
EXEMP - ex-employee
PHYDEST - physical destruction
TINV - theft of inventory
TINFO - theft of information
DATADEST - data destruction
FIN - financial institution
GOVT - government institution
TRANUTIL - transportation and utilities
COMPSERV - computer service company
SALMFC - sales and manufacturing

(a) Inventory manipulation schemes used to disguise thefts;

(b) "Salami tactics" where amounts of money small enough to be viewed as statistical discrepancies are continuously diverted until many thousands of dollars are collected; and

(c) "Trojan horse* programs* usd to erase data and either gain control over an operating system or crash an operating system.

(2) The high losses suffered by computer service companies, transportation and utility companies, and educational institutions probably reflect the greater opportunity for computer crime that confronts employees in these industries. Existence of such opportunities, plus bright individuals, will often lead to system penetration.

(3) Since the estimated probability of incarceration of a computer criminal, given discovery and apprehension, is only .014, computer crime is clearly an attractive proposition.

5. DRUG THEFTS

5.1 Data Description

The data on drug thefts were made available by the Drug Enforcement Administration (DEA). They include information on quantities of drugs stolen by employees of drug manufacturers and distributors, drug types, street prices of these drugs, information on the number of drug audits and investigations performed by DEA, and information on the number and types of sanctions imposed for infractions of regulatory code. Data on some variables cover the period

*A program clandestinely placed in the operating system which, when triggered by 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. (Such a tactic could be used in a reactor sabotage scenario or against an automated material control and accounting system.)

from the third quarter of 1973 to the first quarter of 1978 for each of the 13 DEA regulatory districts.* Other data series (street prices, for example) were available for shorter periods. Information on quantities of drugs of various types that were reported by DEA as "lost in transit" is also included.

5.2 Analog Value

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

5.3 Data Limitations

As was mentioned earlier, the drug data were available only as aggregates, not on a case-by-case basis. Two other weaknesses of the data set should be mentioned:

(1) Street Prices - This information was 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 across locations can be high. The price data point used, for a given time period, is the average of these purchases. Since not enough purchases are made to provide price

*Since the acquisition of these data, DEA's regulatory districts have been reorganized into five regions.

information by region, the price information available for each quarter may be viewed as a rough estimate of the national "average" price for the particular drug.

(2) Quantities Stolen - conversations with DEA agents indicate that a substantial portion of total drug thefts go undetected. Of those that are detected, there exist powerful incentives on the part of managers to cover up shortages.*

5.4 Analysis

(1) High black market prices provide incentives to insiders to engage in risky illegal activities.

(2) Increases in the use of mild sanctions (warnings, letters of admonition and administrative hearings) relative to more severe measures for infractions (inventory seizure, arrest) actually have incentive effects on perpetrators and potential perpetrators of the illegal activity.

(3) Reasonable measures of enforcement and penalty severity are negatively related to associated illegal activity levels.

(4) Quantities of drugs "lost in transit" increase with the street price of the same drug. This observation is consistent with the conviction of many DEA agents that such "lost" drugs are in fact stolen.

(5) Although only 2% of all cases of drug thefts involve insiders, they represent almost 20% of total losses (Employee Pilferage, Table B.23).

5.5 Conclusions

The LLL study draws the following conclusions on the analog between drug thefts and potential nuclear crime:

*LLL notes that these are the same incentives that may lead to inventory difference cover-ups in the nuclear industry, viz., desire to avoid regulatory sanctions, Freedom of Information suits, and undesirable publicity.

Table B.23

Drug Losses from Manufacturers and Distributors
by Type of Incident--Relative Importance, 1973-77*

Units of Measurement \ Type of Incident	Night Break In	Armed Robbery	Employee Pilferage	Customer Theft	Lost in Transit	Other Thefts
Number of Incidents ÷ Total of Incidents	.023	.006	.020	.021	.657	.264
Dosage Units Stolen ÷ Total Dosage Units Stolen	.062	.015	.195	.012	.542	.171

* Total number of cases with data on both variables is 247.

(1) Since 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), periods of high and rising SNM (black market) prices should be viewed as periods when special vigilance is required.

(2) Drug thieves and potential drug thieves view their activities in much the same way as those engaged exclusively in legal activities. This has especially ominous implications for organized crime if black market prices of SNM rise enough to overshadow returns from drugs, prostitution and other mainstays of organized crime.

(3) If federal regulatory code designates a series of sanctions for code infractions, policymakers should be aware that increasing the use of perfunctory sanctions may, all other things being equal, actually lead to increases in the activity the sanction was designed to curtail.

(4) Increasing enforcement (as measured by the number of arrests in the drug cases) has an unambiguous deterrent effect on illegal activity.

(5) Since a large portion of all drugs "lost in transit" are probably stolen and since the number of such cases is 33 times larger than the number of cases in which insiders are involved in a drug theft, it appears 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.

APPENDIX C

NUCLEAR EVENTS

The following list is comprised of instances in which an insider operated against a nuclear-related target. It is not intended to be a complete catalog of insider crimes in the nuclear industry, but a selected list of events for which complete and meaningful data were available and in which there was definite insider involvement. (For a more exhaustive list of all types of nuclear-related events involving NRC licensees, see NUREG-0525, the Safeguards Summary Event List.)

1. Surry Nuclear Power Station
Surry, VA

On May 7, 1979, two plant operator trainees, both of whom were employed at the site for approximately one year, entered the fuel storage building, which was locked and alarmed, and poured sodium hydroxide on 62 of 64 new fuel assemblies being stored there. One individual acted as a lookout while the other ripped open the plastic protective liners and vandalized the fuel. Both were authorized access to the storage building. Their stated motivation was to demonstrate security laxity at the site.

Access to the building was controlled by use of a coded keycard, which electronically unlocks the alarmed personnel portals. Coded keycards were issued to both licensee and contractor personnel after successful completion of a fairly comprehensive background screening program that included criminal and credit record checks, a check of the applicant's previous seven years of employment, and a reference check.

In addition, site management certified monthly that each individual with a keycard still needed access to the storage building in order to perform required duties.

As a result of this event, access controls were tightened.

2. General Electric
Wilmington, NC

On January 29, 1979 the General Manager of the facility received an extortion letter and a sample of uranium oxide (UO_2) powder. The letter stated that the writer had in his possession two five-gallon containers of UO_2 low enriched powder which he had taken from the plant. The containers were identified in the letter by serial number and by their gross weight and totalled approximately 145 pounds. The letter further stated that enough UO_2 had been removed from one of the containers to furnish samples to newspaper editors, senators, anti-nuclear group leaders and others if the writer's demand for $100,000 in cash was not met by February 1. The writer also said that if his demands were not met, a container of UO_2 powder would be dispersed through an unnamed, large, American city. The UO_2 powder from the second container would be dispersed through yet another large city if an additional $100,000 in cash were not provided.

The General Manager verified the authenticity of the container numbers and the fact that the containers were not in their assigned location. (The fact that two containers were missing was established by the licensee's control and accounting system, independently and simultaneously with the General Manager's receipt of the extortion letter.)

The FBI assumed investigative jurisdiction on January 29, 1979. On February 1, 1979, a temporary employee of a General Electric subcontractor was arrested.

The employee, who had been employed approximately one year, confessed to the crime and was subsequently convicted and sentenced to 15 years in prison.

3. NUMEC
Leechburg, PA

The perpetrator, a plant employee, worked in the metals building where source material and depleted uranium were processed at the site. He claimed that in the late 1960's he removed from the site an oak crate he wanted, which was identified for disposal. When he got the crate home and opened it, he discovered that it contained what he believed was depleted uranium, mostly metal scrap, odds and ends in various shapes and sizes. Among these items was what appeared to be a gallon paint can, which he believed contained some sort of uranium oxide. The individual hid the material in the rafters of his basement because he was afraid to return it to NUMEC.

In early 1971, the individual's radiation badge revealed an abnormally high level and he consented to a survey of his home for possible contamination. No contamination was found, but the material he had hidden in the basement rafters was located.

An analysis of the material identified it as 35 pounds of depleted uranium and less than three grams of high enriched uranium. The manner in which the material was removed from the site is unknown, nor is it known how the high enriched uranium had been mistakenly introduced into the metals building, an area where high enriched uranium was prohibited.

4. Argonne National Laboratory
Chicago, IL

On May 9, 1975, a calibration standard containing 0.5 grams of plutonium was discovered missing from its storage container. The standard was last seen and handled on May 2, 1975. Security for the building was required to be commensurate with good business practices, i.e., doors locked between 7 p.m. and 5 a.m. and all day on weekends and holidays. During these times the building was patrolled by guards.

An exhaustive search yielded negative results. After an extensive investigation, it was concluded that: 1) the standard had been stolen for unknown reasons; and 2) storage and handling procedures for the standard within the building were inadequate. Possible motives included embarrassment to the Laboratory or to the individual responsible for the standard, removing the standard as a prank or for a souvenir, or to make a point about the SNM control system. No prosecutable evidence was ever developed.

5. Bradwell Nuclear Power Station
Essex, England

A theft of 20 fuel elements containing approximately 400 pounds of natural uranium occurred in mid-November 1966. Two perpetrators, a rigger who worked at the power station and a painter/van driver who had no connection with the station, were involved in the theft. They alleged that an individual offered to pay for the elements on delivery. The alleged buyer was never identified.

The rigger returned to the station during the night after his normal working hours. He stole keys to the storage area and removed the elements on a dolly to a remote area of the station where he threw them over the

fence. The driver was waiting at the fence with a van. The two loaded the elements into the van where they remained until the police recovered them. The fact that the theft had occurred and the location of the stolen elements were revealed by an informant.

Although the perpetrators claimed that money from the sale of the elements was their motivation, it was also speculated that embarassment may have been a motivating factor since an International Atomic Energy Agency inspection had just been completed at the site and all had been found in order.

6. Massachusetts Institute of Technology (MIT)
Boston, MA

On July 1, 1969, four depleted uranium plates weighing 2.45kg were reported lost along with 20 grams of highly enriched uranium. These materials were subsequently found on the desk of an MIT professor following police questioning of a suspect. The consensus of opinion among MIT personnel knowledgeable of this incident was that access to the material was probably gained through the use of an unauthorized MIT master key. (As a result of this event, material was subsequently stored in a lead safe, and the locks on the door leading to the storage area and safe were changed so that they were no longer a part of the Institute's master lock and key system. Locks leading to the reactor area were also changed.) A graduate student at MIT was the prime suspect, but prosecution was not sought due to lack of evidence.

7. Uranium Mining/Milling Operation
Southwest US

In 1979, two mill workers at a uranium mining and milling operation in the Southwest stole seven barrels containing from 900 to 1000 lbs of yellowcake each. The two employees loaded the yellowcake into unnumbered, discarded barrels, transferred the barrels by forklift onto a company truck and drove the truck to a rented U-Haul at a perimeter gate. After transferring the material to the U-Haul, they drove away from the facility.

The two workers had been offered an undetermined amount of money by an outsider to steal the material. They had undergone a routine check of references, but no police check was made. They had been employed two and three years respectively. The theft was detected by means of a tip to federal investigatory authorities.

APPENDIX D

GLOSSARY OF TERMS

Analogous Industry - an industry that protects high value or high risk items or information against insider theft and/or sabotage and that employs safeguards systems that are similar to those required of NRC licensees.

Characteristics - the distinctive features, traits or qualities that distinguish one type of insider adversary behavior from another. For purposes of this study, the following 17 adversary characteristics were considered: target control, screening, access, length of service, training/skill level, training/skill relevance, stimulus, motivation, dedication, insider group size, outsider involvement, equipment usage, equipment availability, crime type, role, planning and tactics.

Computer Crime - a crime that either directly or indirectly involves a computer system as a means or as a target in the perpetration of the crime.

Conspiracy/Collusion - secret agreement, understanding or cooperation between two or more individuals for an illegal or deceitful purpose; may involve individuals inside and outside a plant or facility.

Detection - the initial means by which the occurrence of a crime is discovered.

Embezzlement - appropriation of property, money or information entrusted to one's care fraudulently to one's own use.

Fraud - intentional perversion of truth in order to induce another to part with something of value.

Full-Field Background Investigation - a personally conducted investigation to obtain full facts about the background and activities of a person so that it can be determined if his employment with the U.S. Government is consistent with the interest of national security; the basic elements of a full-field

investigation are: (1) a national agency check (FBI fingerprint and investigative files, Office of Personnel Management investigative files, and House Committee on Internal Security plus a check with State Department's passport files); (2) personal interviews with present and former employers, supervisors, fellow workers, references, neighbors, school authorities and other knowledgeable associates; and (3) checks of police, credit (when practical and justified), and other pertinent records, as appropriate (FBI field offices, military service, etc.) (Source: Federal Personnel Manual.)

Insider - a person recognized and accepted as having authorized access to a facility or activity.

Material Access Area (MAA) - any location that contains special nuclear material within a vault or a building, the roof, walls and floor of which each consititutes a physical barrier.

Material Balance Area (MBA) - an identifiable physical area into and out of which the quantity of nuclear material being moved is represented by a measured value determined through an NRC-approved measurement and measurement control program.

Material Control and Accounting (MC&A) - the part of a safeguards system that encompasses measures, procedures, controls and management to control nuclear material (govern movement and use, monitor inventory and process status, assign and exercise responsibility, and maintain vigilance) and to account for nuclear material (measure, maintain records, provide reports, and perform data analysis).

Radiological Sabotage - any deliberate act directed against any plant or transport activity licensed by NRC or against a component of such a plant or transportation activity that could directly or indirectly endanger public health and safety by exposure to radiation (10 CFR Part 73.2).

Sabotage - any act or omission of an act that maliciously causes the destruction of property or information or disrupts the operations of a facility or activity.

Safeguards - those measures designed to guard against radiological sabotage and the theft of nuclear material such as source material and SNM from uses permitted by law, and to give timely indication of possible theft or credible assurance that no theft has occurred.

Security System Vulnerability - any weakness or combination of weaknesses in a security system that facilitates perpetration of insider theft or sabotage.

Special Nuclear Material (SNM) - plutonium, the isotope uranium-233, or the element uranium enriched in the isotope uranium-233 or in the isotope uranium-235.

Strategic Special Nuclear Material (SSNM) - the isotope uranium-235 (contained in uranium enriched to 20% or more in the uranium-235 isotope), the isotope uranium-233, or plutonium.

Theft* - intentional, unauthorized removal of money, material or information from its owner or designated custodian.

Vital Area - any area that contains any equipment, system, device or material, the failure, destruction or release of which could directly or indirectly endanger the public health and safety by exposure to radiation; the walls roof and floor of a structure containing such vital equipment constitute physical barriers.

*For purposes of the study, the term "diversion," the intentional removal of money, material or information from uses permitted by law or treaty, is subsumed under theft.

Acronyms and Initials

ABA	American Banking Association
BF&E	Bank fraud & embezzlement
DEA	Drug Enforcement Administration
DNA	Defense Nuclear Agency
DOD	Department of Defense
DOE	Department of Energy
FDIC	Federal Deposit Insurance Corporation
GACS	Generic Adversary Characteristics Study
ID	Inventory difference
LLL	Lawrence Livermore Laboratory
MC&A	Material control & accountability
NMSS	Office of Nuclear Material Safety and Safeguards (NRC
PAP	Personnel Assurance Program (DOE)
PRP	Personnel Reliability Program (DOD)
SAI	Science Applications, Incorporated
SNM	Special nuclear material
SSNM	Strategic special nuclear material

APPENDIX E

ANALOGOUS INDUSTRIES

For purposes of the study, the industries listed below were deemed most analogous to the nuclear industry. Although the degree of analogy may vary from industry to industry or from facility to facility within each industry, the generic analog remains valid because it is based on two facts: (1) all of the industries manufacture, distribute, transport or in some way handle high value or high risk items; and (2) all have safeguards systems in place to protect such items.

Fifty-nine security representatives of all but three of these industries nationwide were interviewed by the principal study group and its consultants. For the three industries not contacted directly, case history data were obtained from Federal agencies and local law enforcement agencies. The interviews, often more than one per industry, yielded both case history information and expert opinion.

Analogous Industry	Safeguarded Item(s)	No. of Interviews
Money Handlers		
Banking	Money, Creditcards	4
Insurance	Money, Policies	4
Casino	Money	2
Racetrack	Money	1
Other Lending Institutions	Money	1
Trade Associations	Retirement Funds	0
		12
Material Handlers, Manufacturers Distributors		
Aerospace/Aircraft	Proprietary Design Information; Classified Information	7
Oil/Petrochemicals	Oil, Petrochemicals; Proprietary Geological Information	6
Precious Metals and Mining	Ore, Metals; Proprietary Geological Information	4
Arms Manufacturing	Arms	2
Auto Manufacturing	Components; Proprietary Design Information	2
Chemical Manufacturing	High Risk Chemicals	2
Drug	High Value/Risk Drugs	2
Electronics	Components; Proprietary Design Information	2
Museum	High Value Inventory	2
Ordnance Manufacturing	High Value/Risk Ordnance	..
Precious Gem	Gems, Watches, Jewelry	2
Construction	Bidding Information	1

Analogous Industry	Safeguarded Item(s)	No. of Interviews
Material Handlers, Manufacturers, Distributors (Cont'd)		
Department Store	High Value Inventory	1
Softdrink Manufacturing	Proprietary Formulas	1
Telecommunications	Components; Proprietary Design Information	1
Toy Manufacturing	Proprietary Design Information	1
Agriculture	Grain Elevators	0
Clothing	High Value Inventory Including Furs	0
		38
Money/Material Transporters		
Airline	High Value Cargo	4
Armored Car	High Value Cargo	1
Railroad	High Value Cargo	1
Specialized Commodity Carrier	High Value Cargo	1
		7
Other		
Computer Facility	Hardware, Proprietary Software	1
Energy Research Laboratory	Proprietary Design Information; Classified Information	1
		2
	TOTAL	59

APPENDIX F

SPECIAL CASES

As noted in Section 2.6.2.1 (Analog Development), in reviewing the initial data set of 200 cases, we discovered some cases that contained infrequently observed but interesting aspects of insider crime. These aspects are addressed below.

(1) Involvement of Security Personnel

Security personnel present a special problem for safeguards designers since they may require more access or control over a variety of targets than other employees and are likely to be trusted because of their position and authority. In our data base, a total of ten incidents of theft and two of sabotage were perpetrated by security officers, all but three of whom were self-initiated (one was induced by an outsider, one was levered by an insider, and one was unwitting). All served in an operational capacity, and in all but three of the theft cases, they operated alone. One of the exceptions involved collusion among a driver, a guard and a custodian to steal $150,000 from their armored vehicle.

(2) Manipulation of Procedural Tolerances

An insider at a nuclear fuel cycle facility might take advantage of his knowledge of allowable inventory differences to commit multiple, small diversions. In five theft cases, the perpetrators manipulated such tolerances by keeping the amount of money or material stolen within what they knew to be acceptable limits. For example, in one medical insurance fraud, the adjustor/perpetrator, whose company provided health insurance for a number of business firms, kept the amounts of the phony claims he submitted

below $500 because he knew that claims for more than that amount required a more detailed audit. Further, he knew the number of claims a given insuree could file before its insurance rates would be increased and he never exceeded that limit.

(3) Involvement of Former Employees

Should a former employee wish to attempt theft or sabotage, his potential for success compares favorably with other outsiders by virtue of his knowledge of facility operations and personnel. If he bears a grudge against the former employer because of some perceived injustice, he represents an even greater threat.*

Four cases in our preliminary data base involved former employees--two theft and two sabotage.** In one of the sabotage cases, a person who had been fired from his job at a chemical storage site returned to the facility one night two months later, eluded the security patrols, entered the storage yard, and opened the valves on several large chemical storage tanks. Almost 100,000 gallons of chemical agent were drained into a sump and the sewer system, with total damage and product loss equalling $250,000.

(4) Corporate Corruption

The possibility of corruption at the highest levels of a corporation or company represents a serious insider threat that must be considered in the design and implementation of any safeguards system and that argues in favor of independent security components, inventories, audits and inspections. Also, the potential cost of thefts by insiders at this level is higher than than at any other level.

*According to security experts, an employee who knows he is being discharged or laid off is a special threat; he should be watched very closely until the time the discharge occurs. Revenge-driven malevolence during this period is not uncommon.

**These cases were not included for analytical purposes because of their zero analog values.

Within the nuclear industry, for example, a scenario in which corporate management, motivated by company loyalty, manipulates records to conceal material losses or clandestinely maintains material on hand to deal with accountancy anomalies and to avoid fines or closure is not inconceivable.

In eight theft cases and four sabotage (arson-for-insurance) cases, the perpetrators were owners, presidents, vice-presidents, members of the board of directors, or corporate attorneys. For example, several senior executives (president, vice-president and members of the board) of a high value clothing manufacturer engaged in a scheme that involved embezzlement of corporate funds, theft of Small Business Administration funds loaned to the company, diversion of valuable clothing to fences, and defrauding of corporate creditors. The case was brought to the attention of federal investigators by complaining victims and required one year of investigatory work before being broken.

(5) Labor-Related Malevolence

When employees are striking or contemplating a strike or when a union contract is being negotiated, a heightened security posture is recommended because when these conditions exist, otherwise reliable personnel appear more apt to engage in violence or misconduct. Although serious damage and personal injury may not be the intended aims of personnel, they may be the accidental results.

One theft and two acts of sabotage were committed under labor-related circumstances. One of the sabotage incidents, aimed at frightening non-striking truckers into honoring a strike, resulted in manslaughter. Two striking employees of a specialized commodity carrier fired a high-powered rifle at a truck carrying high explosives driven by a scab. Their shots, which

were not intended to hit the cargo, did so. The truck exploded, killing the driver and injuring the perpetrators.

(6) Organized Crime Involvement

Although we found no evidence of organized crime involvement in the nuclear events in the data base, organized crime elements were involved in five analogous incidents (four theft and one arson-for-hire), and attempts by organized crime to gain a foothold in legitimate business by means of infiltration or blackmail are well-documented. Should the intrinsic value of SNM lead to the development of a black market for its illicit sale, the possibility of organized crime participation in such a market may create new challenges for domestic safeguards authorities.

Organized crime was heavily involved, for example, in the Lufthansa heist at Kennedy Airport in 1978. The robbery, which was perpetrated by six outsiders with the assistance of at least one and probably two insiders, netted $9 million worth of currency and jewelry. One of the insiders, a cargo agent, was in considerable debt to bookies associated with organized crime in New York and was threatened with bodily harm unless he provided information on the next high value shipment to be housed at the Lufthansa cargo storage area, detailed plans of the area, keys and combinations. The cargo agent, who was paid $300,000 for his role, apparently co-opted another employee, who was paid $10,000 for his participation. Organized crime elements allegedly planned the robbery, assembled the team, laundered the currency and eliminated several members of the gang who could have led authorities to them. A government informant in the case was discovered missing and is presumed dead.

(7) Large Conspiracies

Five thefts in the overall data base (two analog 2's, one analog 1, and two analog 0's) were perpetrated by 10 or more insiders in collusion. Three involved between 10 and 20 insiders, one involved about 30 insiders, and in the last case, nearly 200 insiders participated in the elaborate Equity Funding Insurance fraud, the largest fraud ever perpetrated in the U.S.

Although the formation of large conspiracies was observed infrequently in our overall data base, the potential for their formation exists, even in a strong safeguards environment, and should be a consideration, not a focus, in the development of a balanced safeguards system.

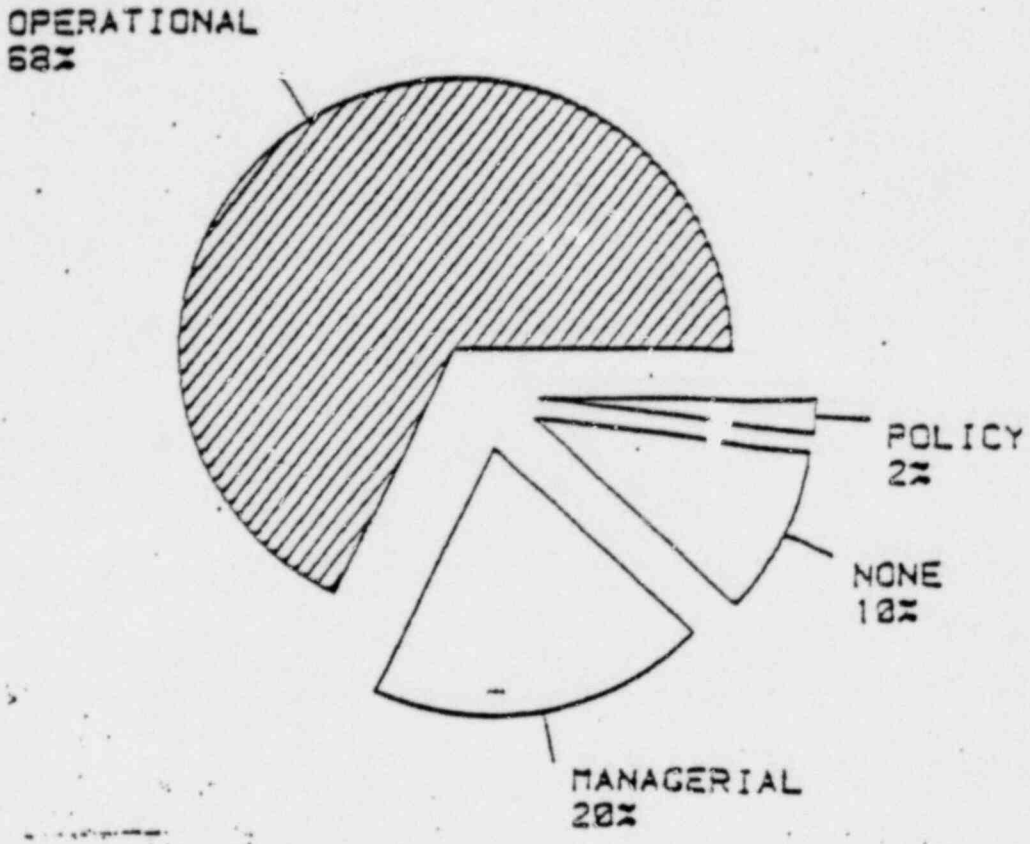
APPENDIX G

FIGURES AND TABLES

This appendix contains all figures and tables referred to in the body of the study.

FIGURE G.1

DISTRIBUTION OF TYPES OF TARGET CONTROL: THEFT, ANALOGS 1&2*



*TOTAL NUMBER OF DATA POINTS FOR THIS CHARACTERISTIC WAS 235.

The following definitions were used:

1. Policy Control - the insider is responsible for determining (controlling) organizational and procedural policy at the victim plant or facility

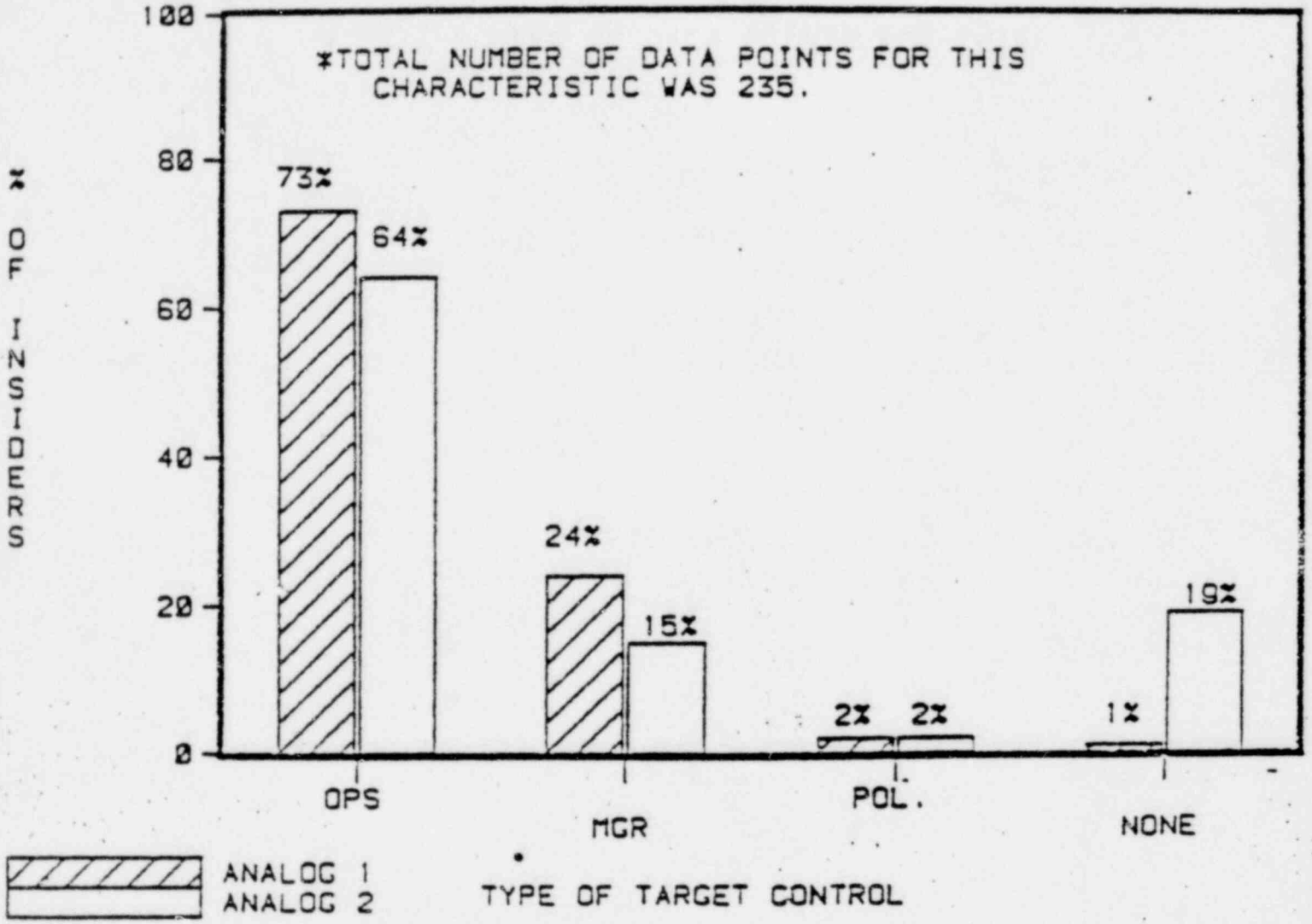
2. Management Control - the insider is responsible for implementing policy (aligns resources, prepares work schedules, etc.; usually a supervisory position) for the targeted activity or site

3. Operational Control - the insider is a non-supervisory line/operations functionary whose routine job duties bring him into contact with the target

4. None - the insider exercised no control over the target

FIGURE G.2

DISTRIBUTION OF TYPES OF TARGET CONTROL: THEFT, ANALOG 1&2 COMPARISON*



The following definitions were used:

1. Policy Control - the insider is responsible for determining (controlling) organizational and procedural policy at the victim plant or facility

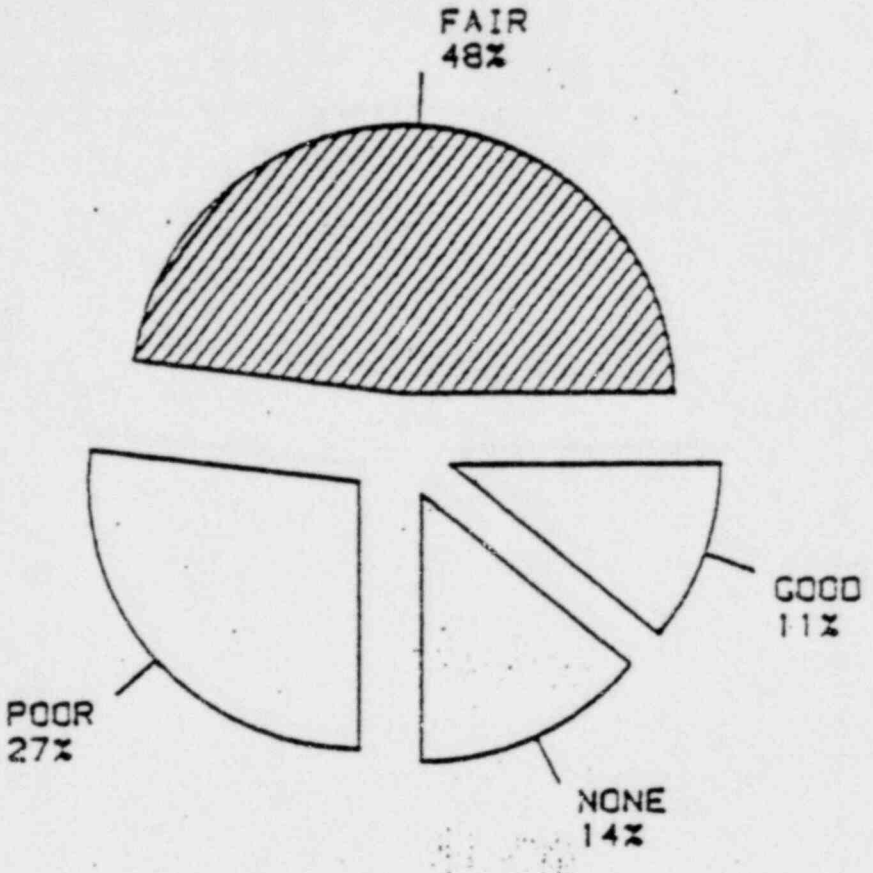
2. Management Control - the insider is responsible for implementing policy (aligns resources, prepares work schedules, etc; usually a supervisory position) for the targeted activity or site

3. Operational Control - the insider is a non-supervisory line/operations functionary whose routine job duties bring him into contact with the target

4. None - the insider exercised no control over the target

FIGURE G.3

DISTRIBUTION OF LEVELS OF SCREENING, THEFT, ANALOGS 1&2*



*TOTAL NUMBER OF DATA POINTS FOR THIS CHARACTERISTIC WAS 169.

The following definitions were used:

1. Good - usually included a full-field background investigation (or its equivalent) and/or a polygraph examination

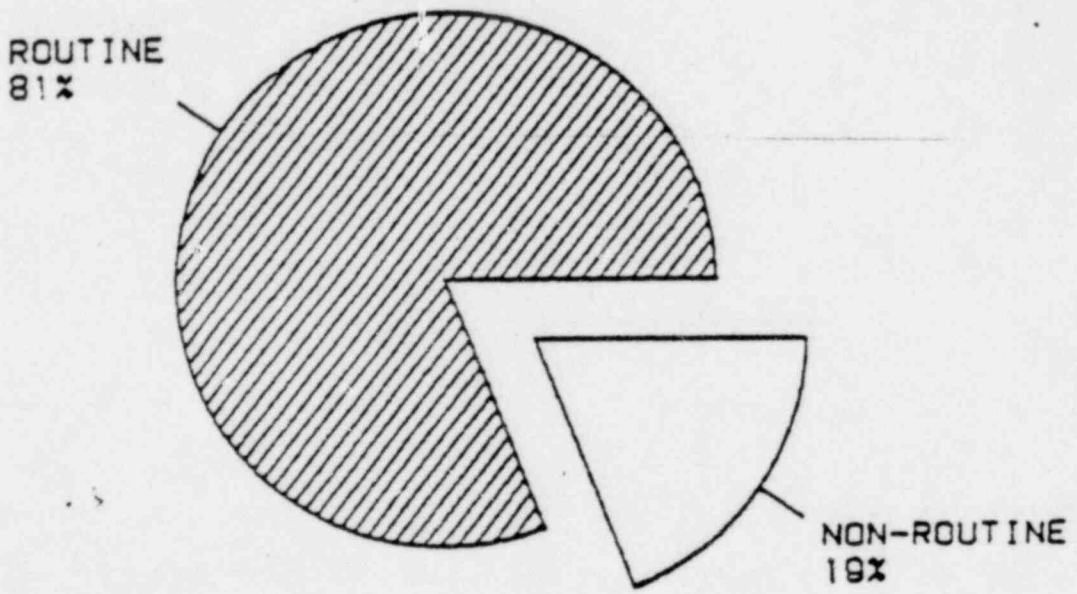
2. Fair - usually included a check with local police, references, and previous employers; might also have included a check with the Department of Motor Vehicles

3. Poor - usually included a check with references or previous employers listed on employment application

4. None - no screening beyond review of employment application

FIGURE G.4

DISTRIBUTION OF TYPES OF ACCESS: THEFT, ANALOGS 1&2*



*TOTAL NUMBER OF DATA POINTS FOR THIS CHARACTERISTIC WAS 235.

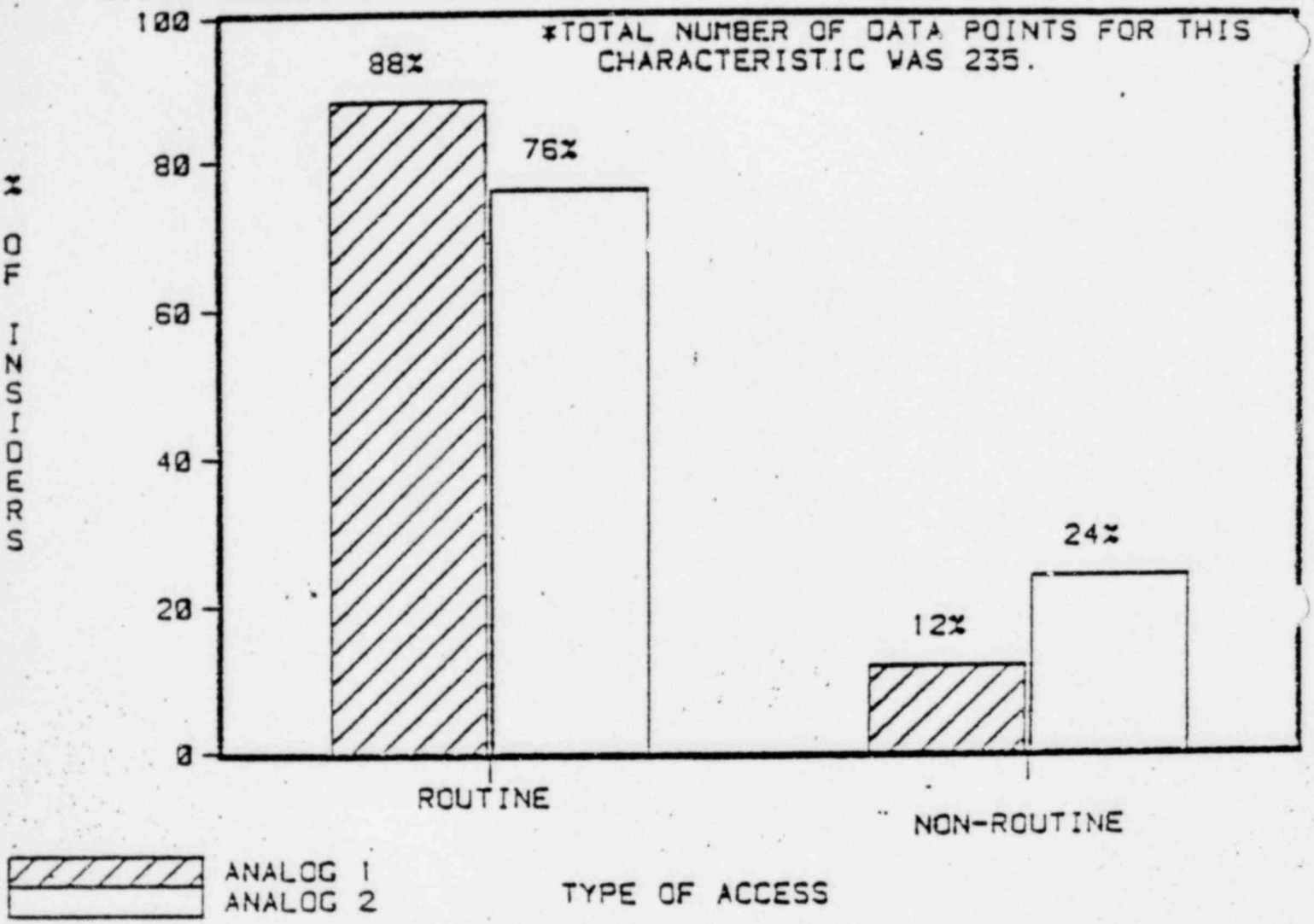
The following definitions were used:

1. Routine - the insider used his normal, authorized access to the target to perpetrate the crime

2. Non-Routine - the insider circumvented or violated some type of access control or gained access to a target that was not part of his normal job duties or routine

FIGURE G.5

DISTRIBUTION OF TYPES OF ACCESS, THEFT, ANALOG 1&2 COMPARISON*



The following definitions were used:

1. Routine - the insider used his normal, authorized access to the target to perpetrate the crime

2. Non-Routine - the insider circumvented or violated some type of access control or gained access to a target that was not part of his normal job duties or routine

FIGURE G.6

DISTRIBUTION OF LENGTH OF SERVICE: THEFT, ANALOG 1&2 COMPARISON*

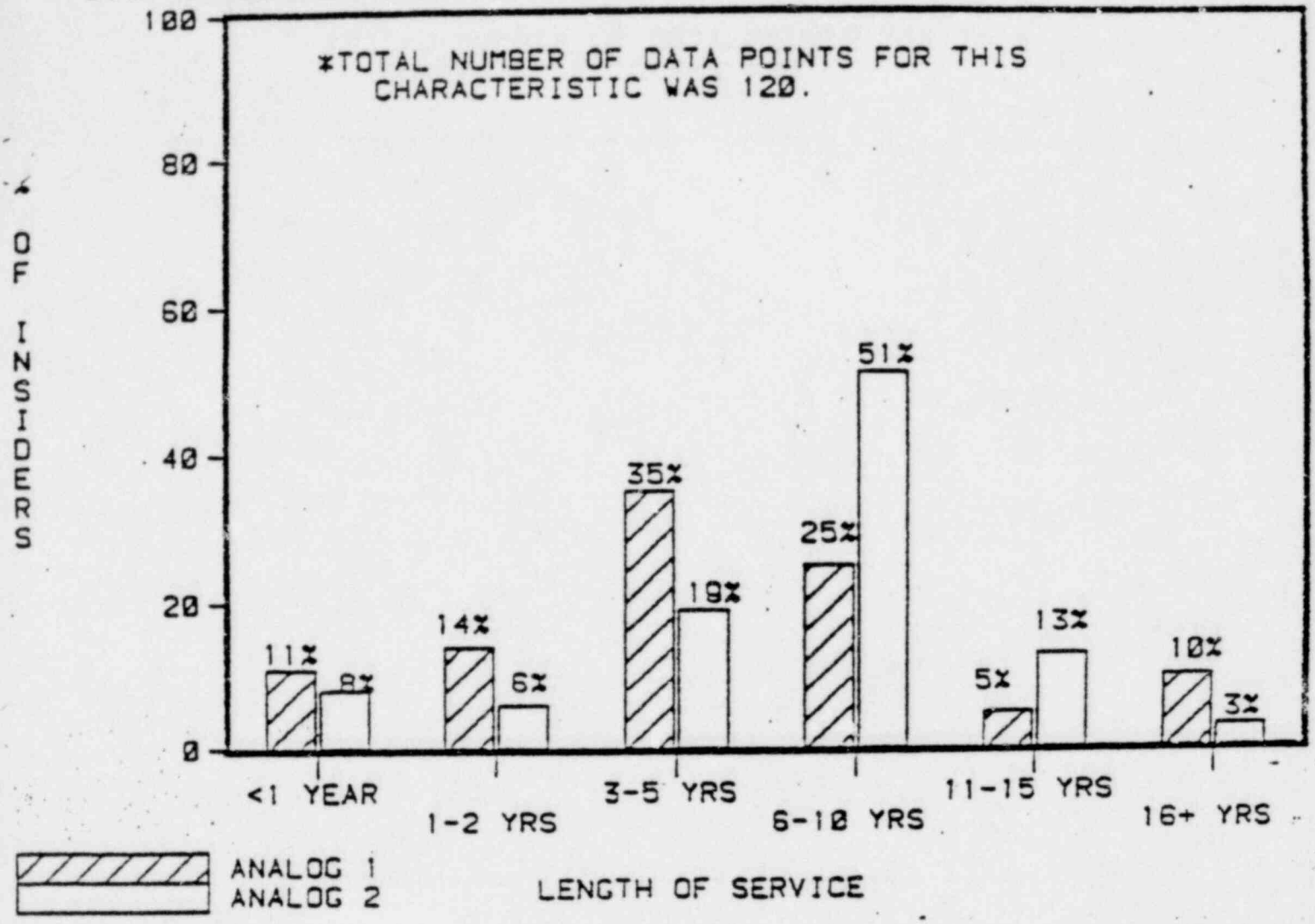
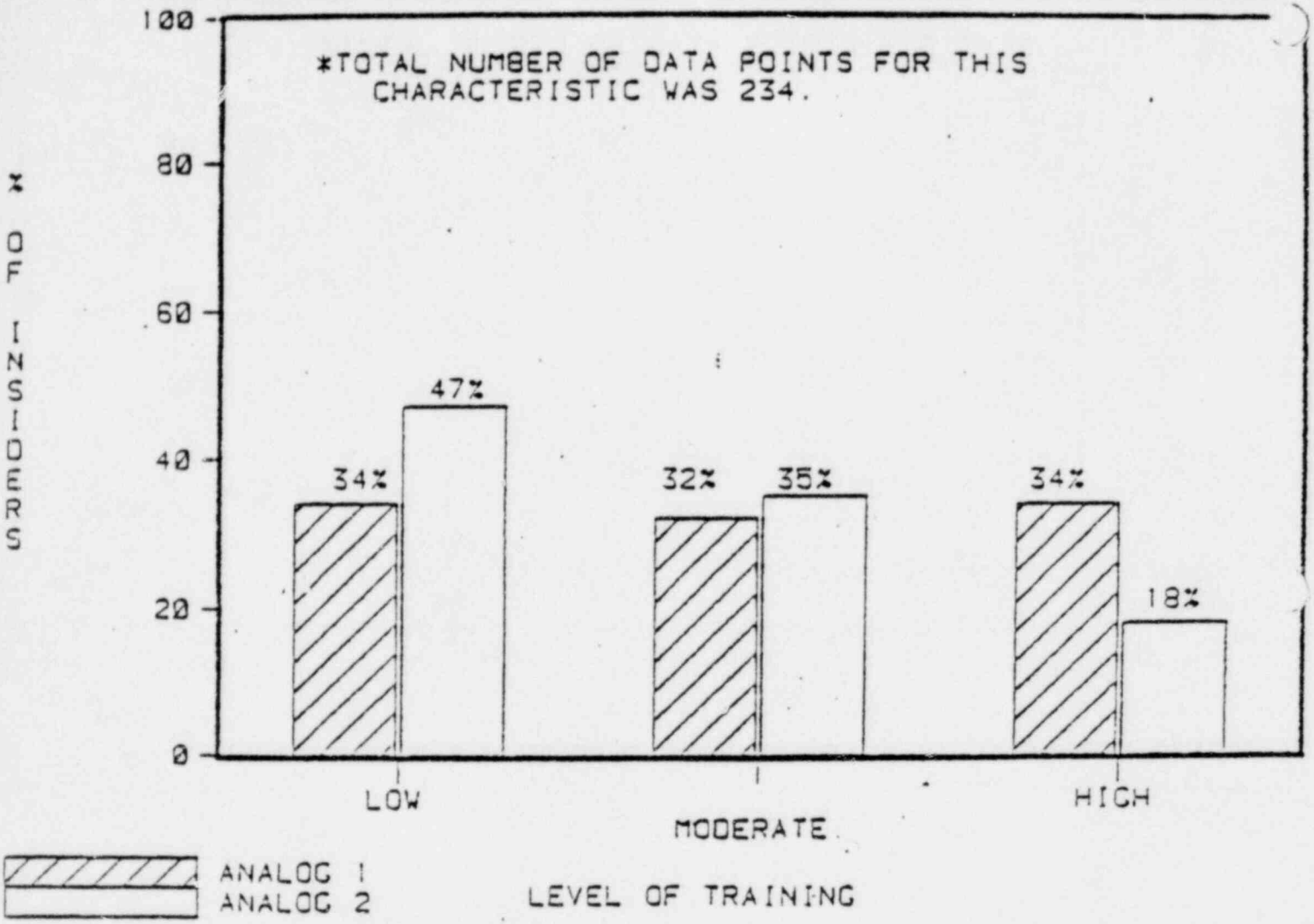


FIGURE G.7

DISTRIBUTION OF LEVELS OF TRAINING: THEFT, ANALOG 1&2 COMPARISON*



The following definitions were used:

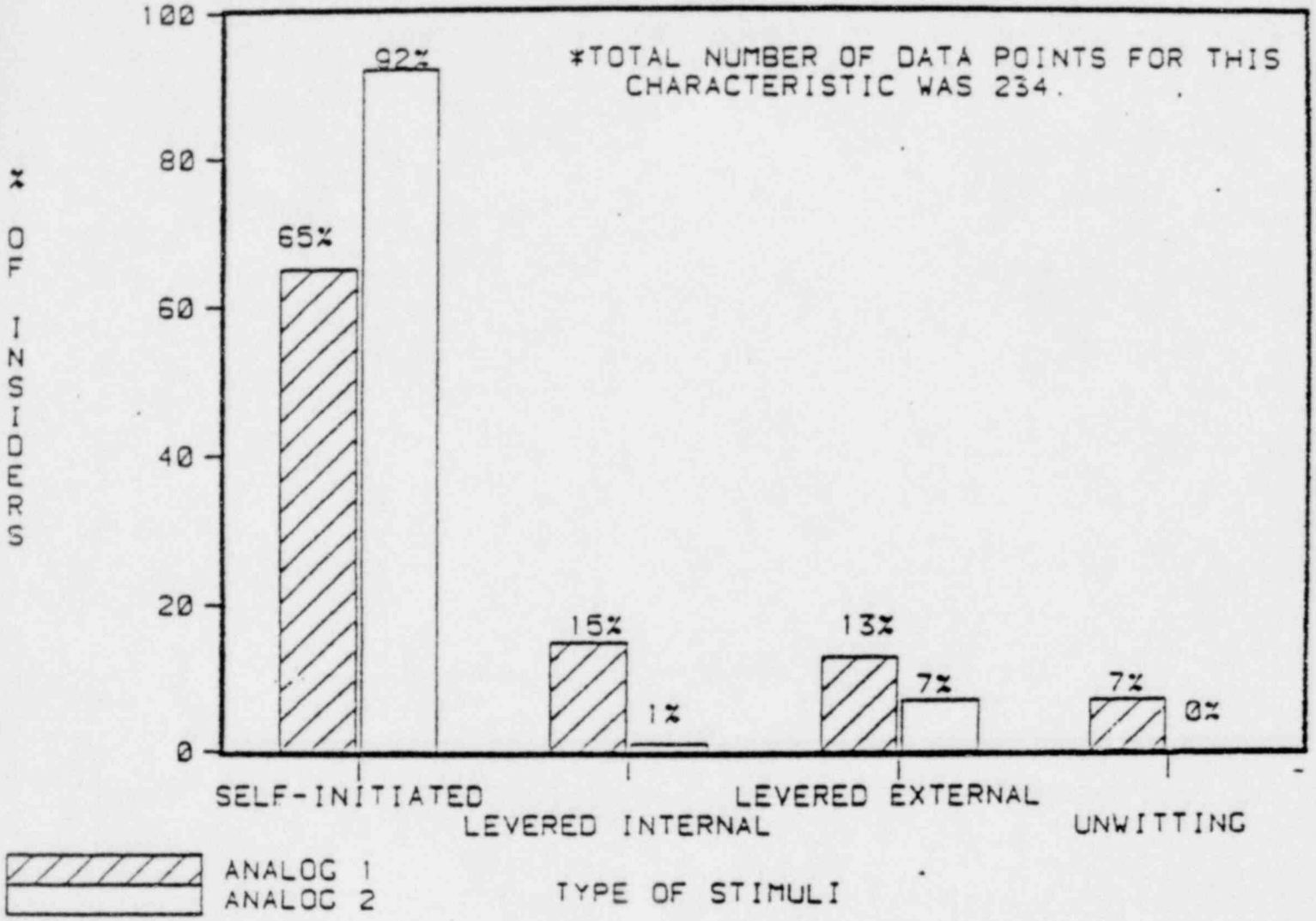
1. Low - the insider occupied a position that required minimal levels of training and skills (e.g., courier, truck driver, production packager, dock clerk)

2. Moderate - the insider occupied a position that required a greater degree of technical expertise and skill development (e.g., bank teller, drug salesperson, computer operator, retail manager)

3. High - the insider occupied a position that required considerable technical training and finely developed skills (e.g., aircraft mechanic, computer programmer, loan officer, intelligence analyst)

FIGURE G.8

DISTRIBUTION OF TYPES OF STIMULI: THEFT, ANALOG 1&2 COMPARISON*

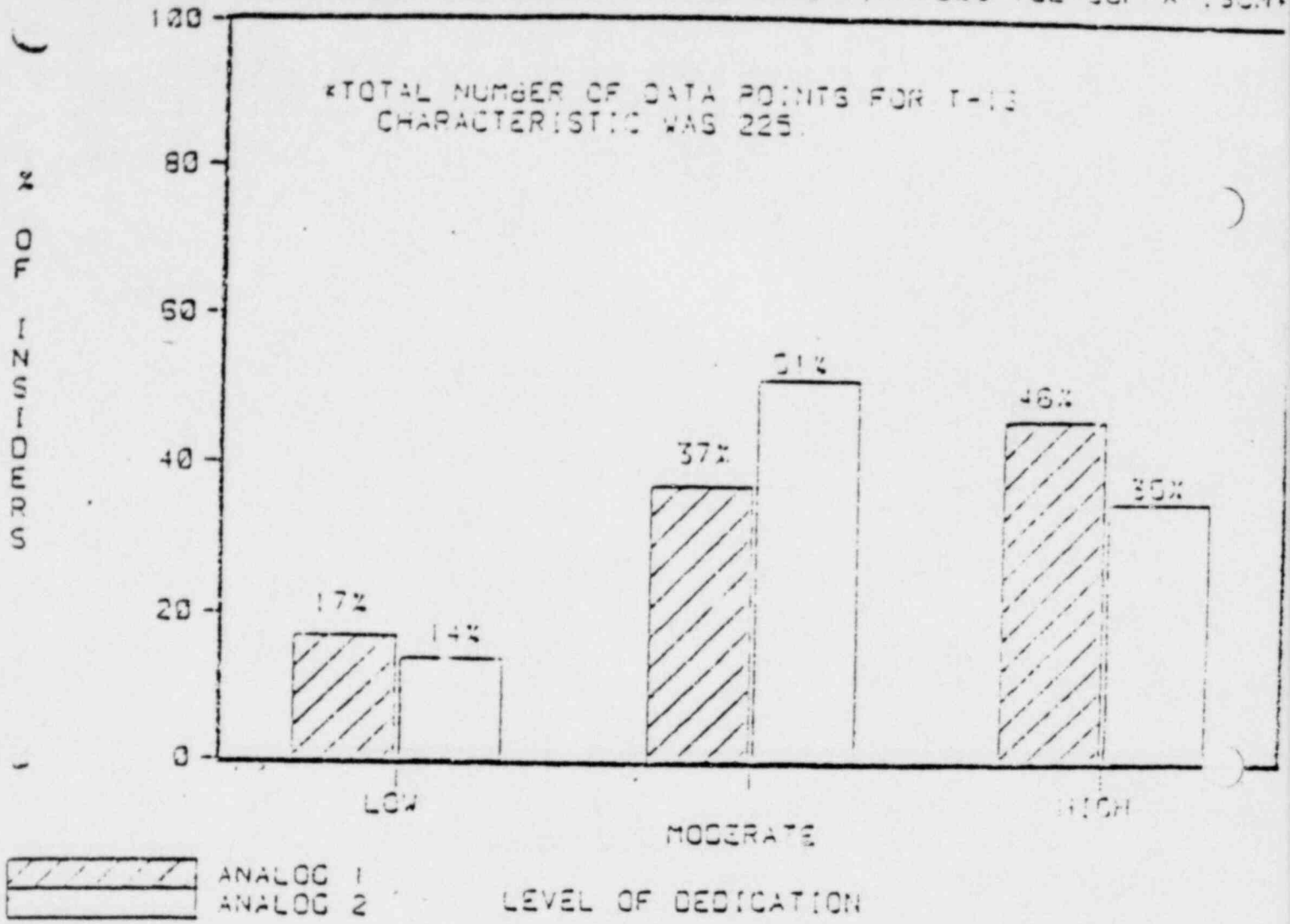


The following definitions were used:

1. Self-initiated - the insider participated in the crime at his own initiation
2. Levered by insider - the insider was persuaded by some inducement or threat offered or made by another insider to participate in the crime
3. Levered by outsider - the insider was persuaded by some inducement or threat offered or made by someone external to the targeted facility or activity to participate in the crime
4. Unwitting - the insider contributed in some way to the commission of the crime, but was unaware of his involvement in a criminal activity

FIGURE G.9

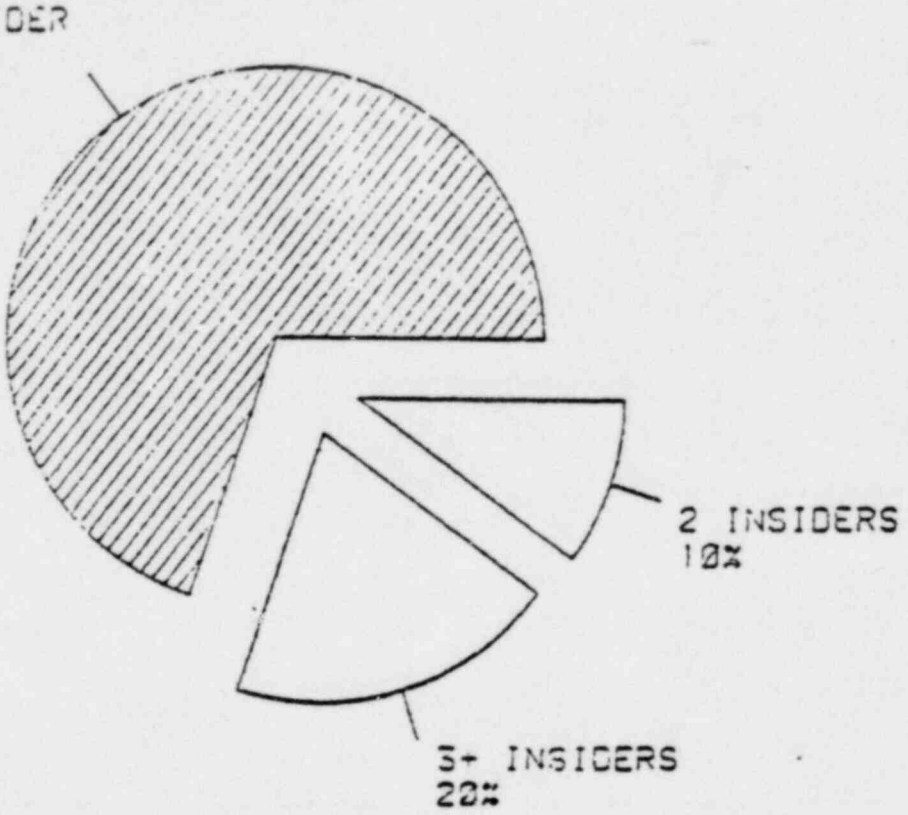
DISTRIBUTION OF LEVELS OF DEDICATION: THEFT, ANALOG 1&2 COMPARISON*



Dedication is defined as the insider's willingness to perpetrate or continue to perpetrate the crime, despite the risks.

FIGURE G.10

DISTRIBUTION OF INSIDER GROUP [illegible] NLOCS 1&2*



*TOTAL NUMBER OF DATA POINTS FOR THIS CHARACTERISTIC WAS 112.

FIGURE G.11

DISTRIBUTION OF INSIDER GROUP SIZE: THEFT ANALOG 1&2 COMPARISON*

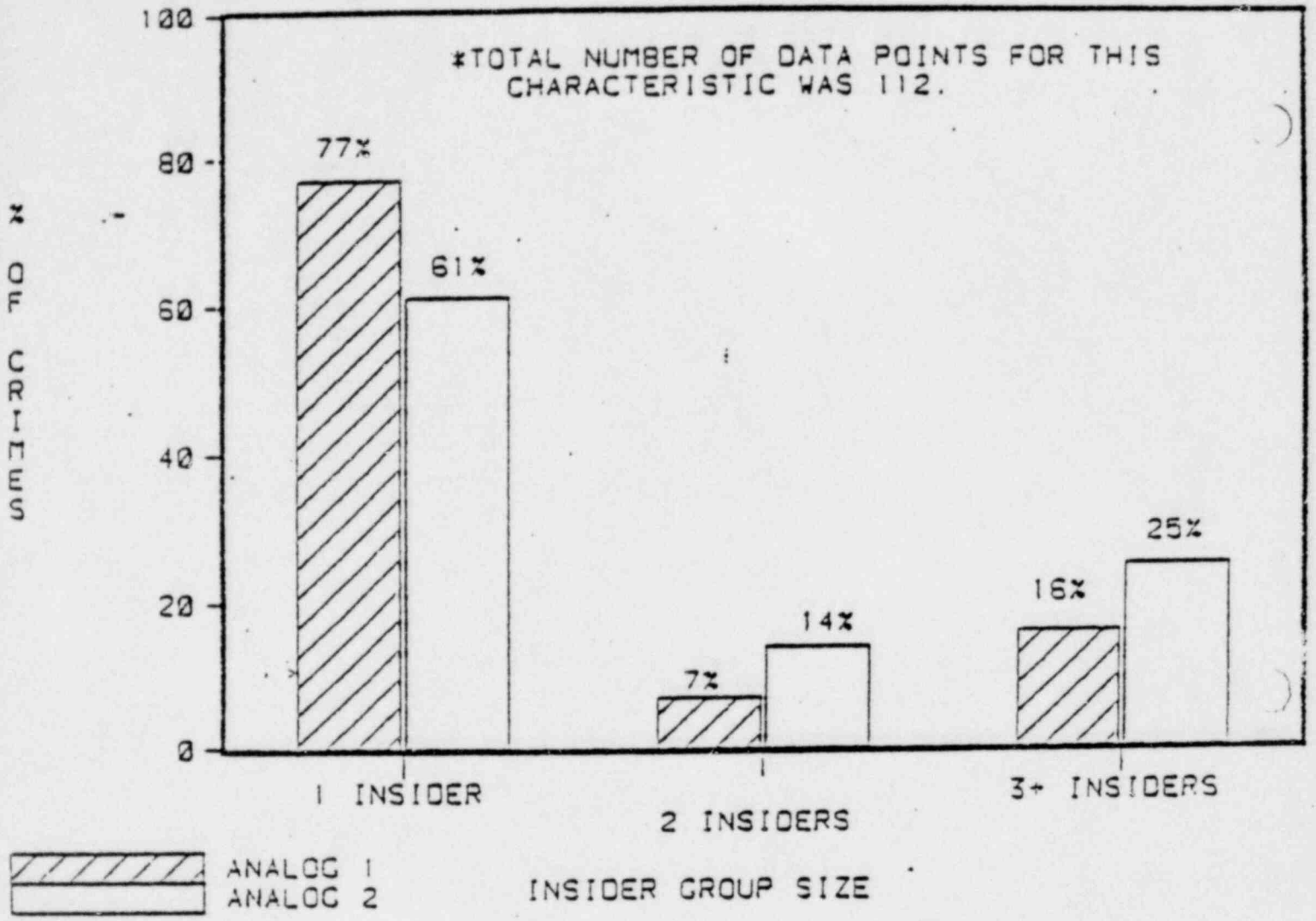
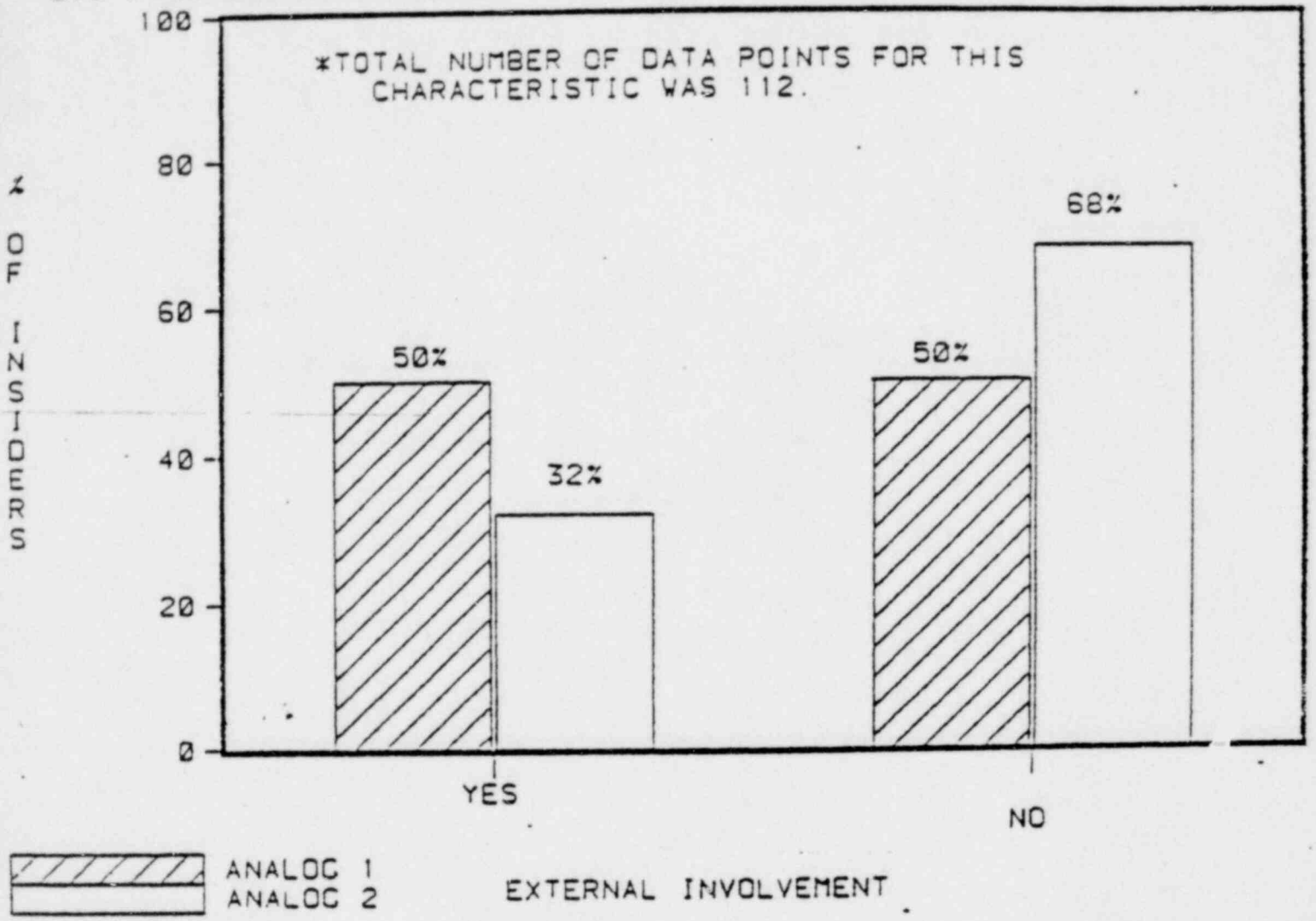


FIGURE G.12

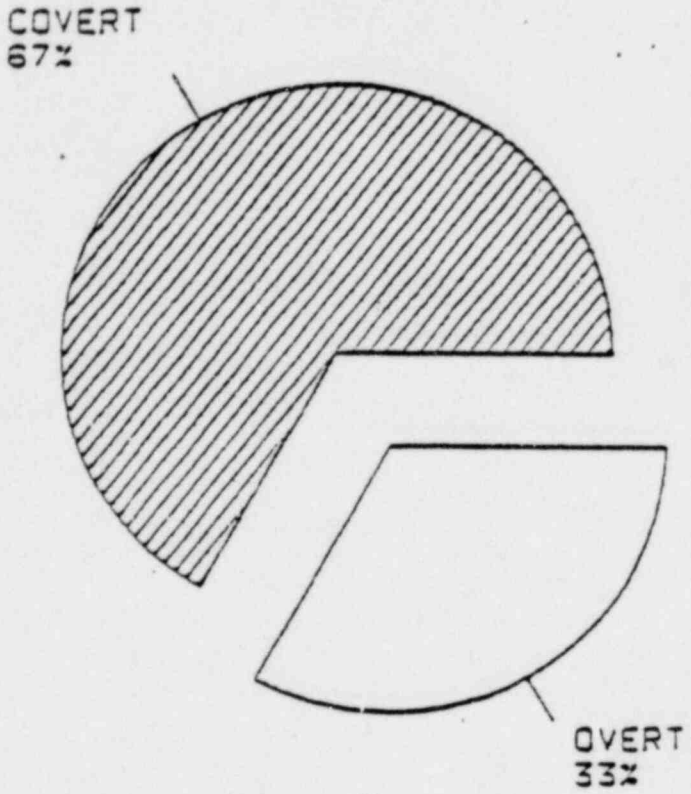
DISTRIBUTION OF OUTSIDER INVOLVEMENT: THEFT, ANALOG 1&2 COMPARISON*



Outsider involvement means that a person(s) not formally associated with the targeted facility participated in the crime in some way.

FIGURE G.13

DISTRIBUTION OF TYPES OF ROLE THEFT, ANALOGS 1&2*



*TOTAL NUMBER OF DATA POINTS FOR THIS CHARACTERISTIC WAS 237.

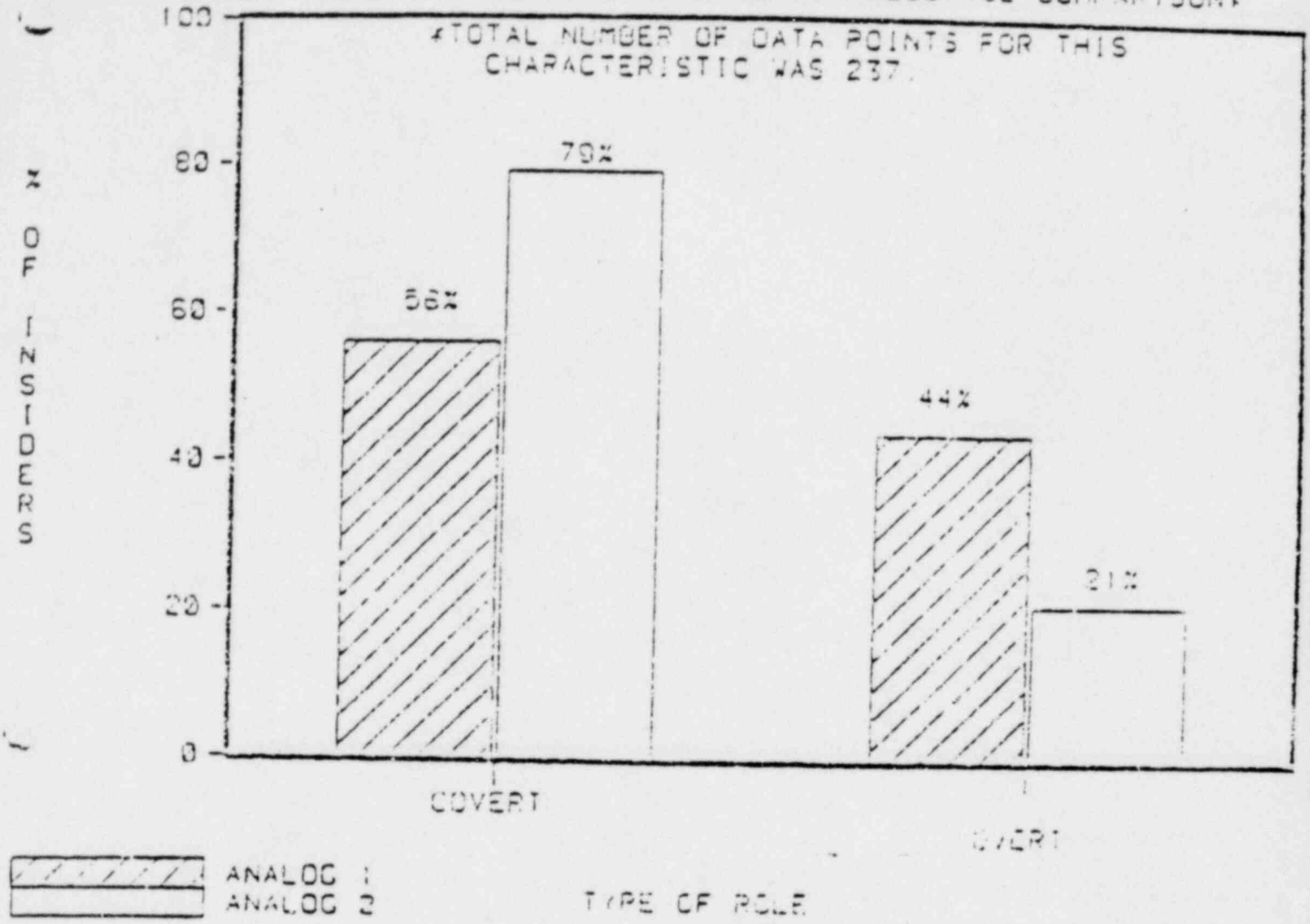
The following definitions were used:

1. Overt - the insider was able to perpetrate the crime in the presence of others without arousing suspicion

2. Covert - the insider was unable to perpetrate the crime in the presence of others without arousing suspicion

FIGURE G.14

DISTRIBUTION OF TYPES OF ROLE THEFT, ANALOG 1&2 COMPARISON*



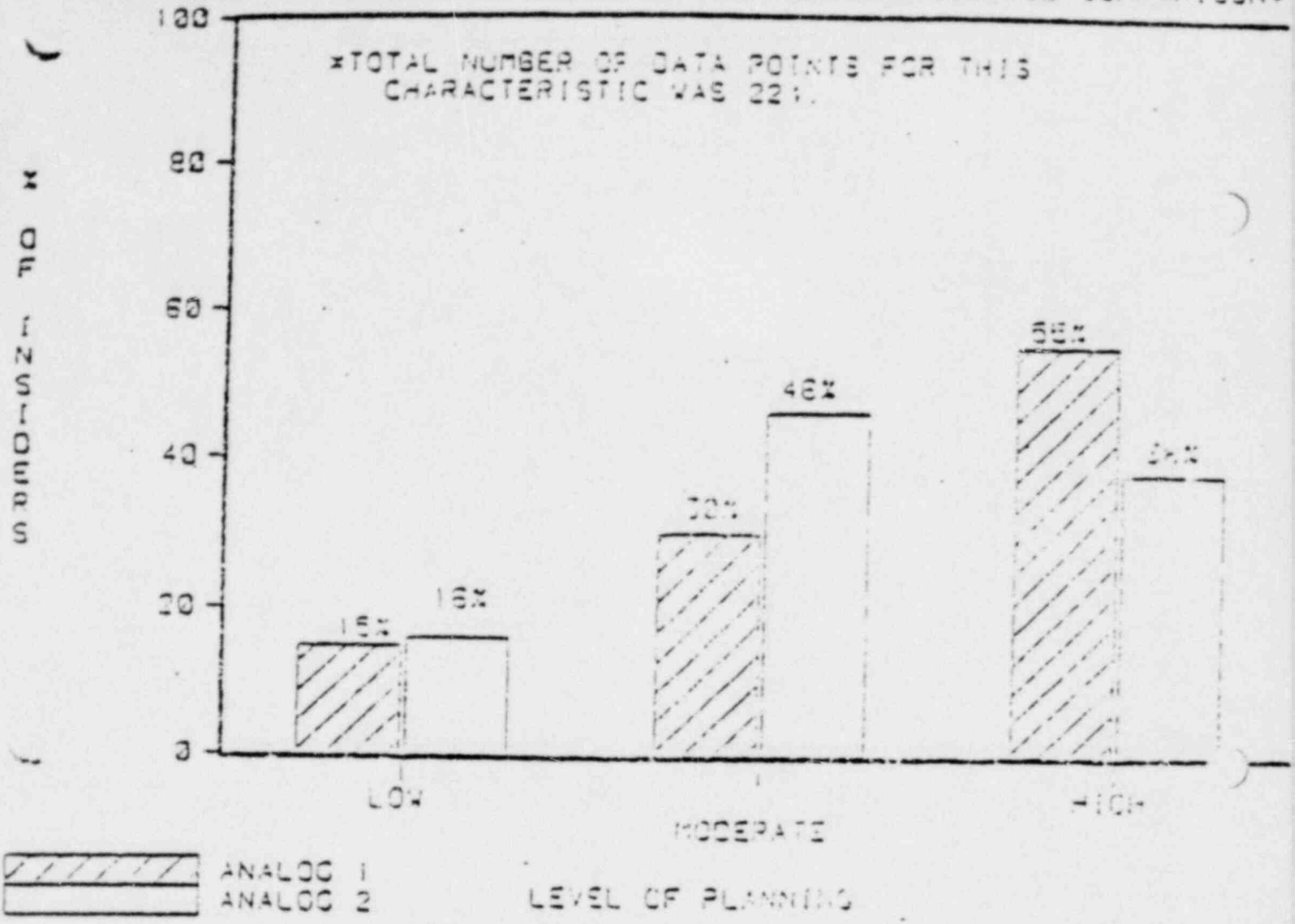
The following definitions were used:

1. Overt - the insider was able to perpetrate the crime in the presence of others without arousing suspicion.

2. Covert - the insider was unable to perpetrate the crime in the presence of others without arousing suspicion.

FIGURE G.15

DISTRIBUTION OF LEVELS OF PLANNING: THEFT, ANALOG 1&2 COMPARISON*



The following definitions were used:

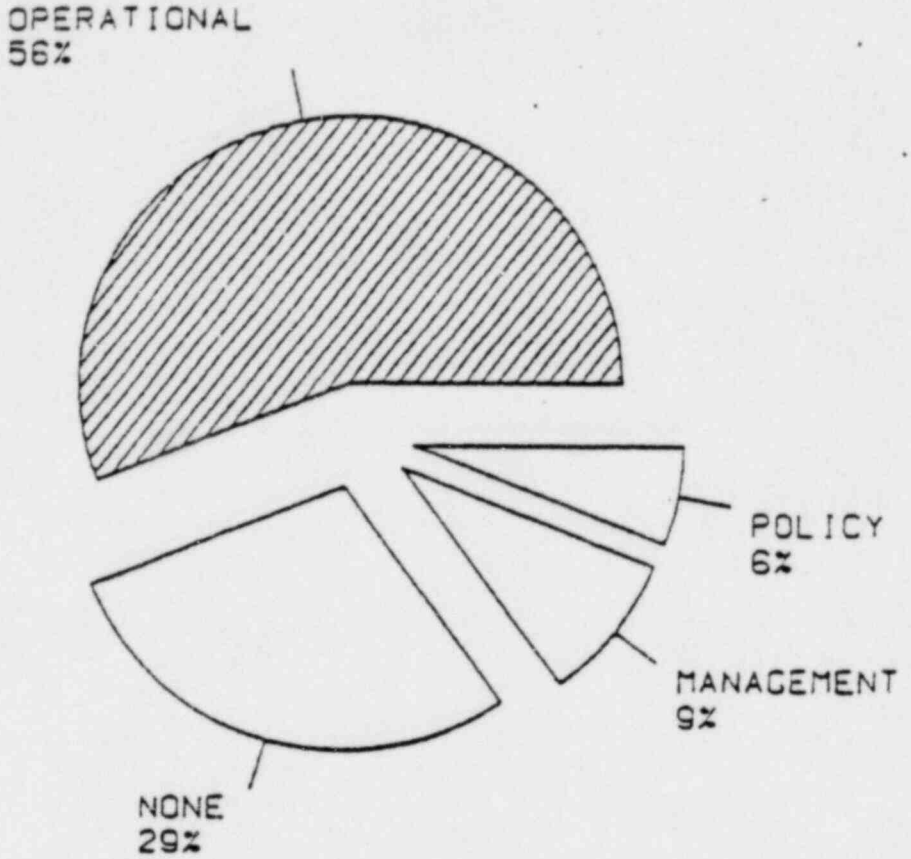
1. High - the insider planned the crime thoroughly and precisely.

2. Moderate - the insider planned for the crime, but with less attention to detail.

3. Low - very little planning was revealed; the crime may have been a spur-of-the-moment act executed against a target of opportunity.

FIGURE G.16

DISTRIBUTION OF TYPES OF TARGET CONTROL: SABOTAGE*



*TOTAL NUMBER OF DATA POINTS FOR THIS CHARACTERISTIC WAS 34. INCLUDES ANALOGS 1&2 AND SPECIAL CASES.

The following definitions were used:

1. Policy - the insider is responsible for determining (controlling) organizational and procedural policy at the victim plant or facility

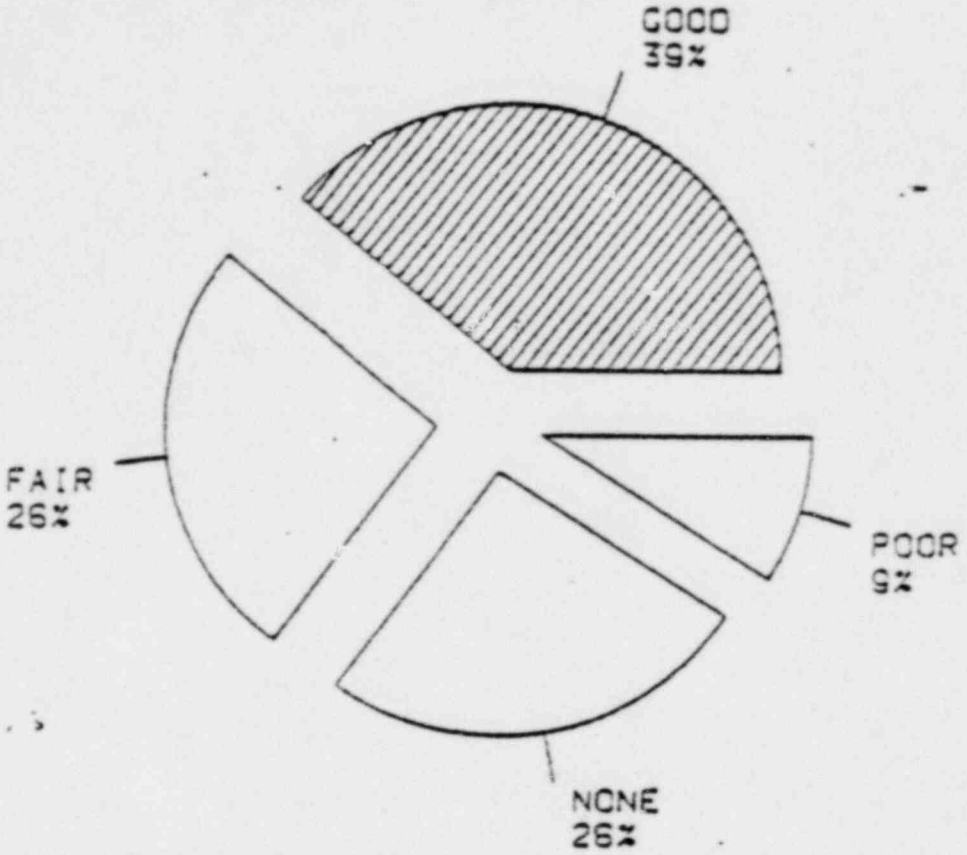
2. Management - the insider is responsible for implementing policy (aligns resources, prepares work schedules, etc.; usually a supervisory position) for the targeted activity or site

3. Operational - the insider is a non-supervisory line/operations functionary whose routine job duties bring him into contact with the target

4. None - the insider exercised no control over the target

FIGURE G.17

DISTRIBUTION OF LEVELS OF SCREENING: SABOTAGE*



*TOTAL NUMBER OF DATA POINTS FOR THIS CHARACTERISTIC WAS 23. INCLUDES ANALOGS 1&2 AND SPECIAL CASES.

The following definitions were used:

1. Good - usually included a full-field background investigation (or its equivalent) and/or a polygraph examination

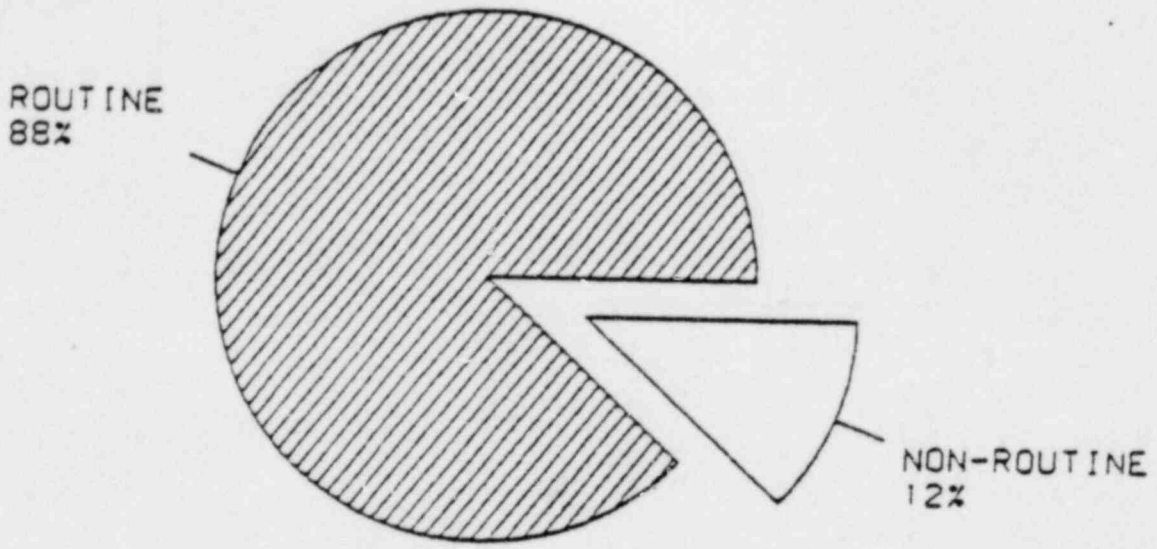
2. Fair - usually included a check with the local police, references, and previous employers; might also have included a check with the Department of Motor Vehicles

3. Poor - usually included a check with references or previous employers listed on employment application

4. None - no screening beyond review of employment application

FIGURE G.18

DISTRIBUTION OF TYPES OF ACCESS: SABOTAGE*



*TOTAL NUMBER OF DATA POINTS FOR THIS CHARACTERISTIC WAS 34. INCLUDES ANALOGS 1&2 AND SPECIAL CASES.

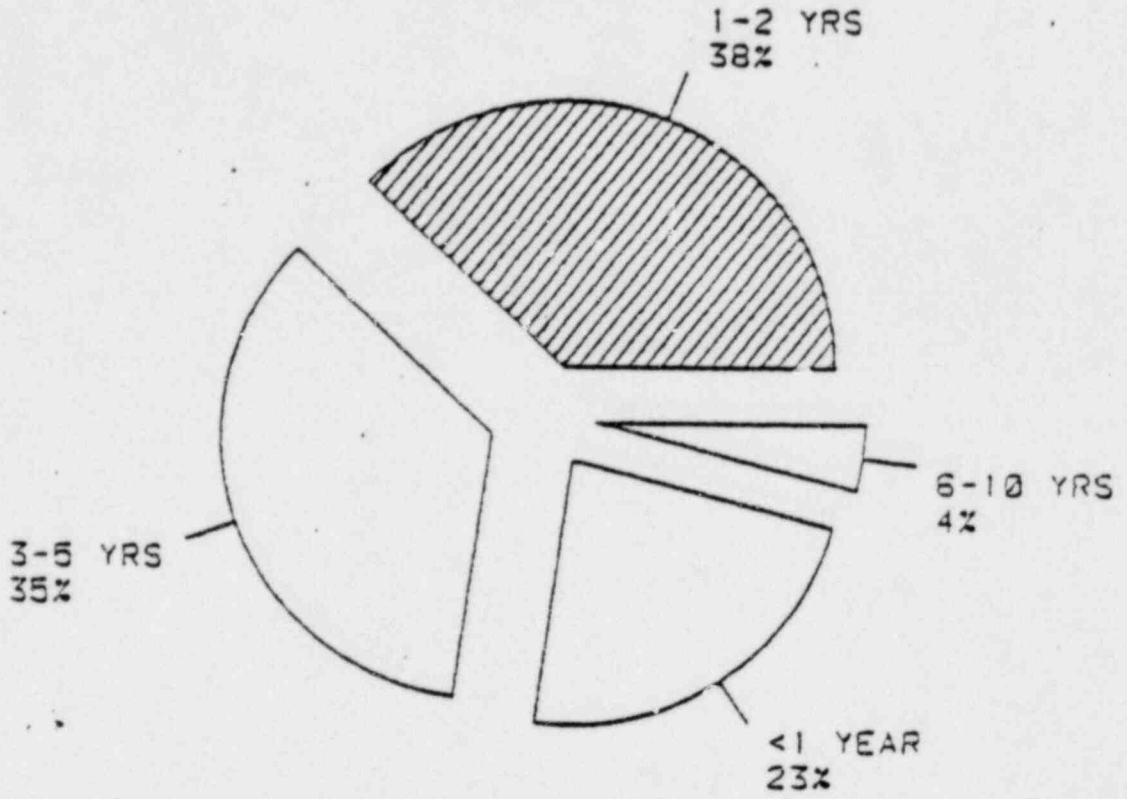
The following definitions were used:

1. Routine - the insider used his normal, authorized access to the target to perpetrate the crime

2. Non-Routine - the insider circumvented or violated some type of access control or gained access to a target that was not part of his normal job duties or routine

FIGURE G.19

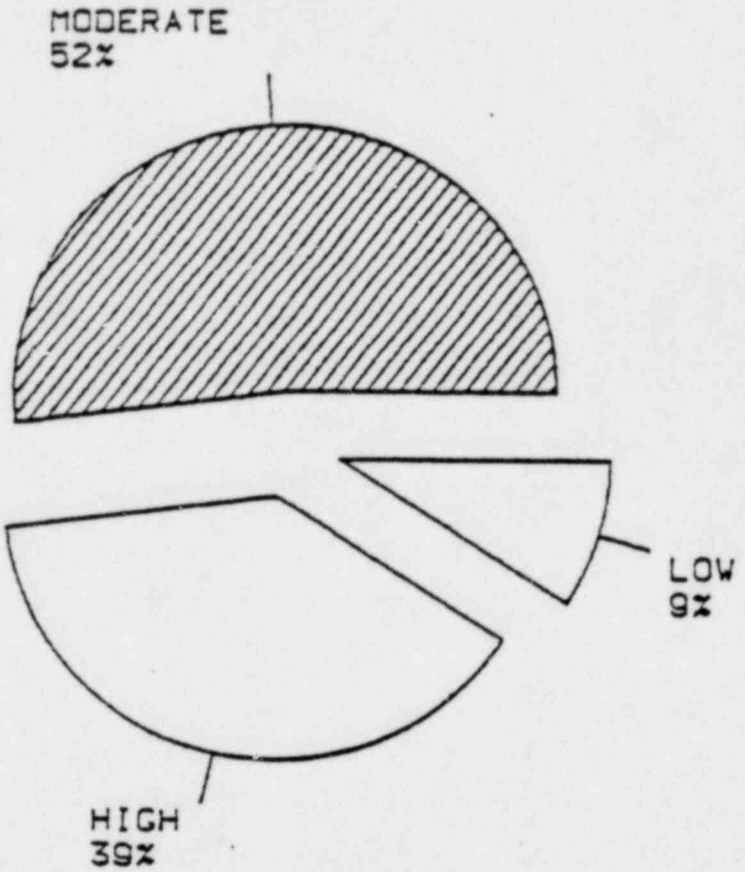
DISTRIBUTION OF LENGTHS OF SERVICE: SABOTAGE*



*TOTAL NUMBER OF DATA POINTS FOR THIS CHARACTERISTIC WAS 26. INCLUDES ANALOGS 1&2 AND SPECIAL CASES.

FIGURE G.20

DISTRIBUTION OF LEVELS OF TRAINING AND SKILLS: SABOTAGE*



*TOTAL NUMBER OF DATA POINTS FOR THIS CHARACTERISTIC WAS 33. INCLUDES ANALOGS 1&2 AND SPECIAL CASES.

The following definitions were used:

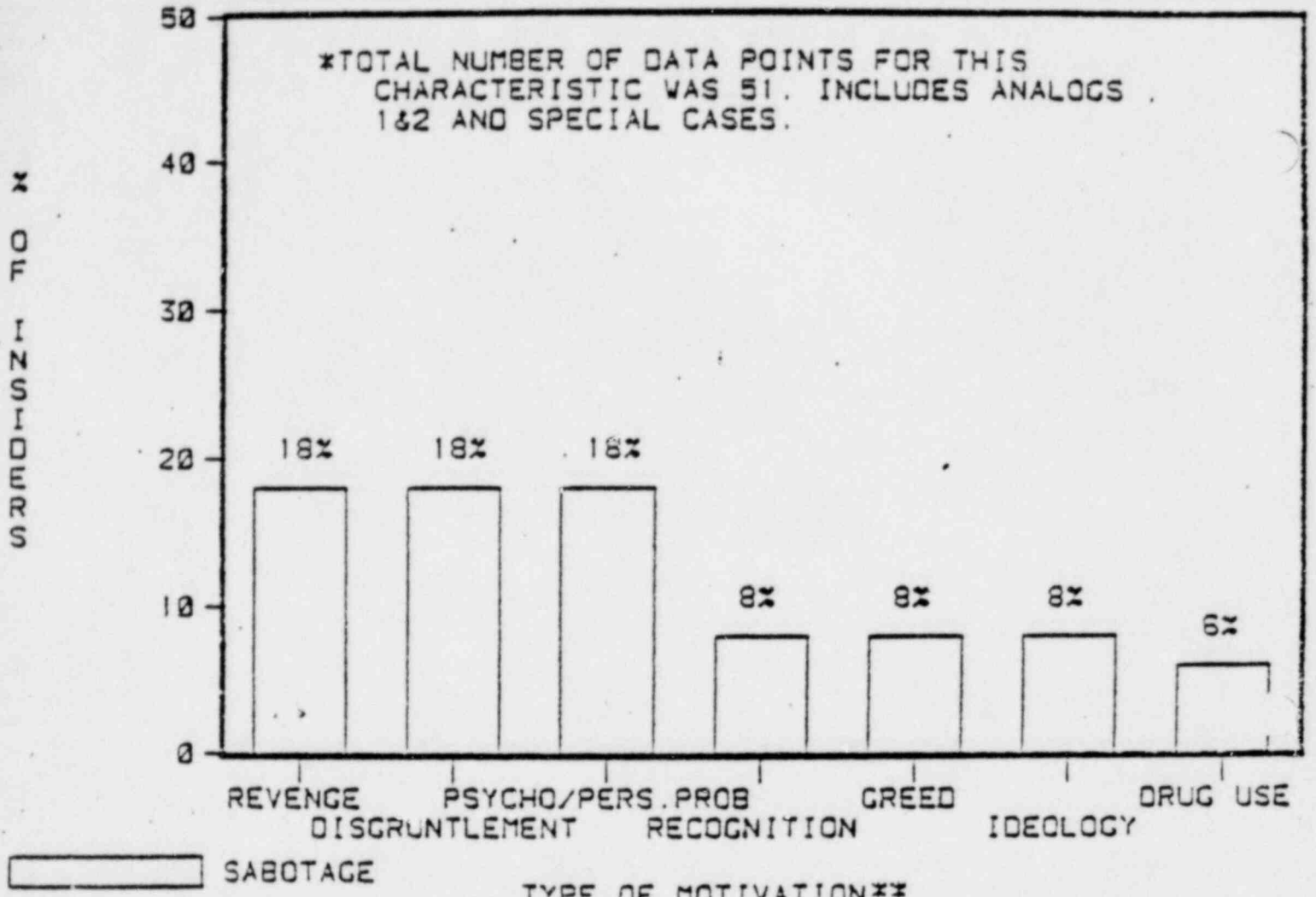
1. High - the insider occupied a position that required considerable technical training and finely developed skills (e.g., aircraft mechanic, computer programmer, loan officer, intelligence analyst)

2. Moderate - the insider occupied a position that required a lesser degree of technical expertise and skill development (e.g., bank teller, drug salesperson, computer operator, retail manager)

3. Low - the insider occupied a position that required minimal levels of training and skills (e.g., courier, truck driver, production packager, dock clerk)

FIGURE G.21

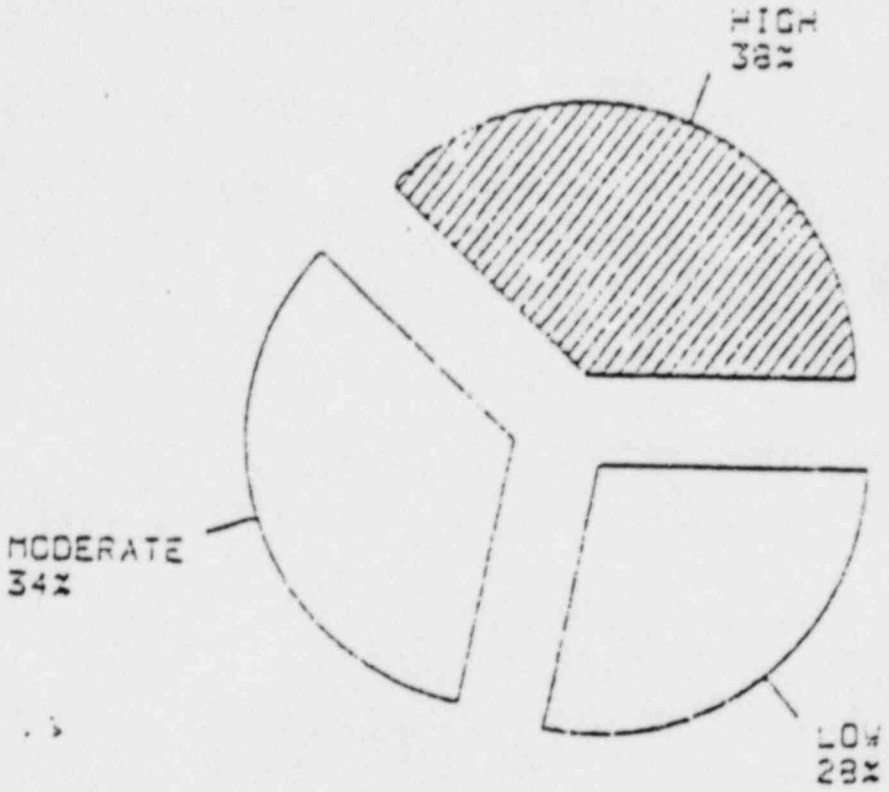
DISTRIBUTION OF TYPES OF MOTIVATIONS: SABOTAGE*



**FOR A COMPLETE LIST OF MOTIVATIONS, SEE TABLE G.14.

FIGURE G.22

DISTRIBUTION OF LEVELS OF DEDICATION, SABOTAGE*

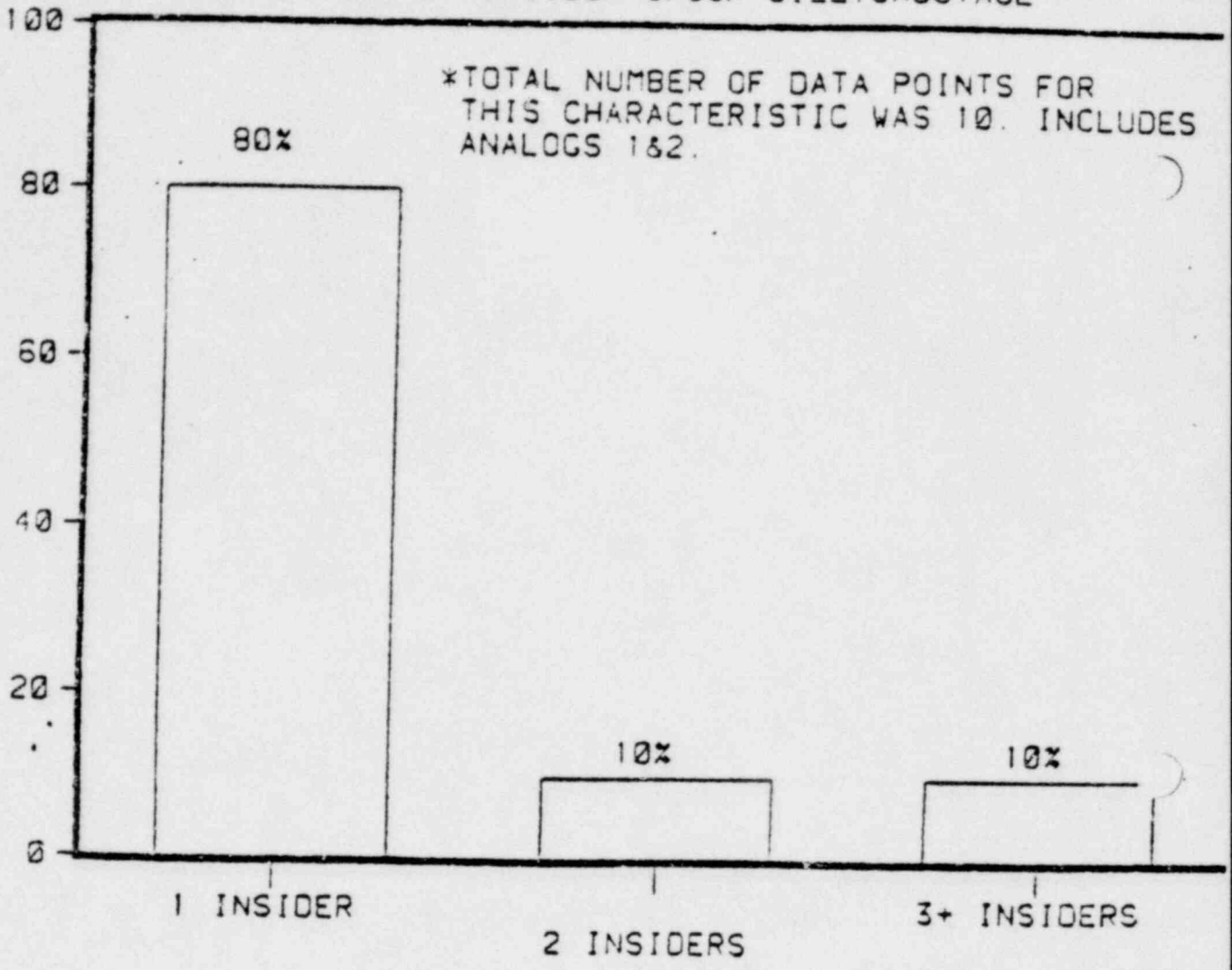


*TOTAL NUMBER OF DATA POINTS FOR THIS CHARACTERISTIC WAS 32. INCLUDES ANALOGS 1&2 AND SPECIAL CASES.

Dedication is defined as the insider's willingness to perpetrate or continue to perpetrate the crime, despite the risks.

FIGURE G.23

DISTRIBUTION OF INSIDER GROUP SIZE: SABOTAGE



G.23

DISTRIBUTION OF INSIDER GROUP SIZE: SABOTAGE

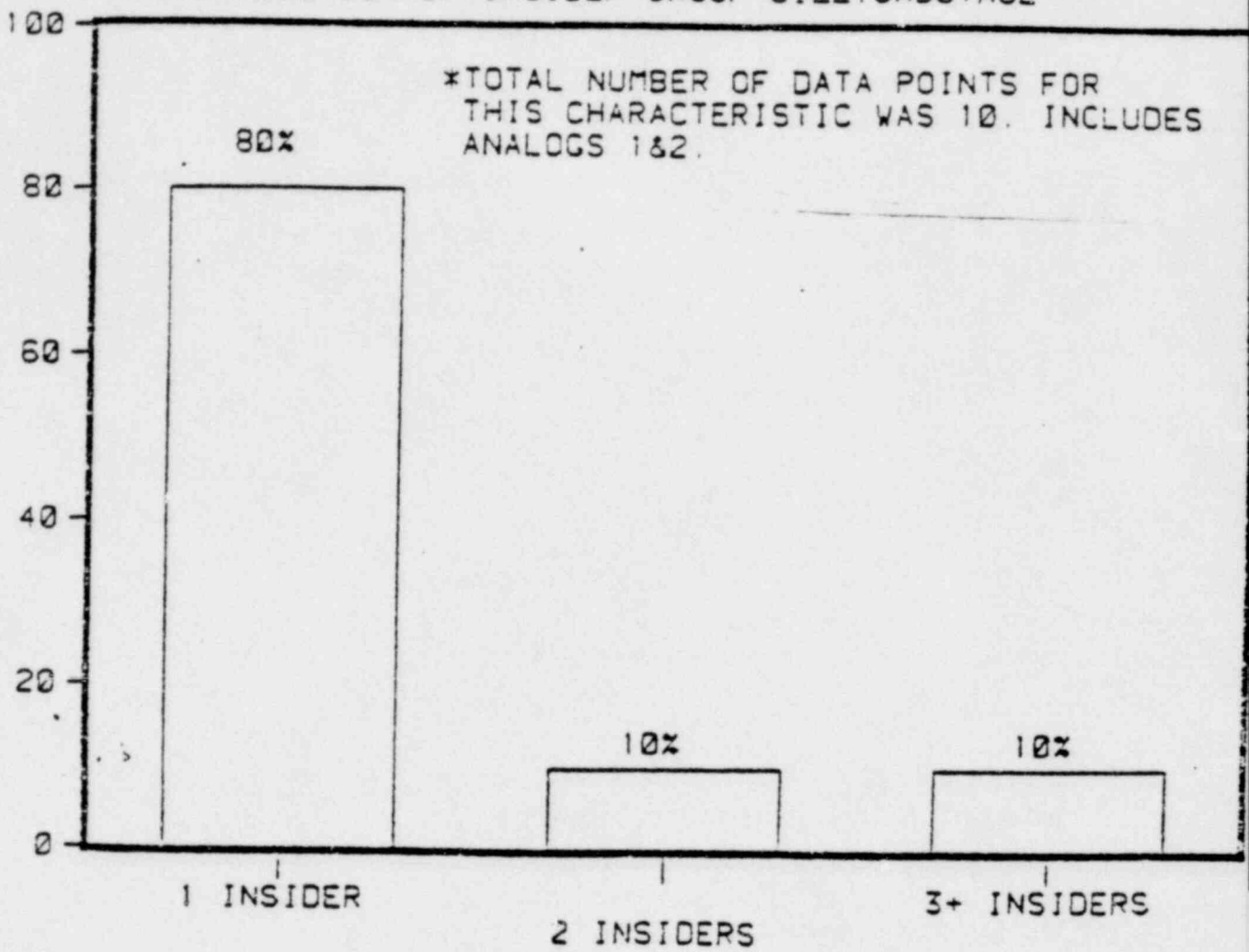
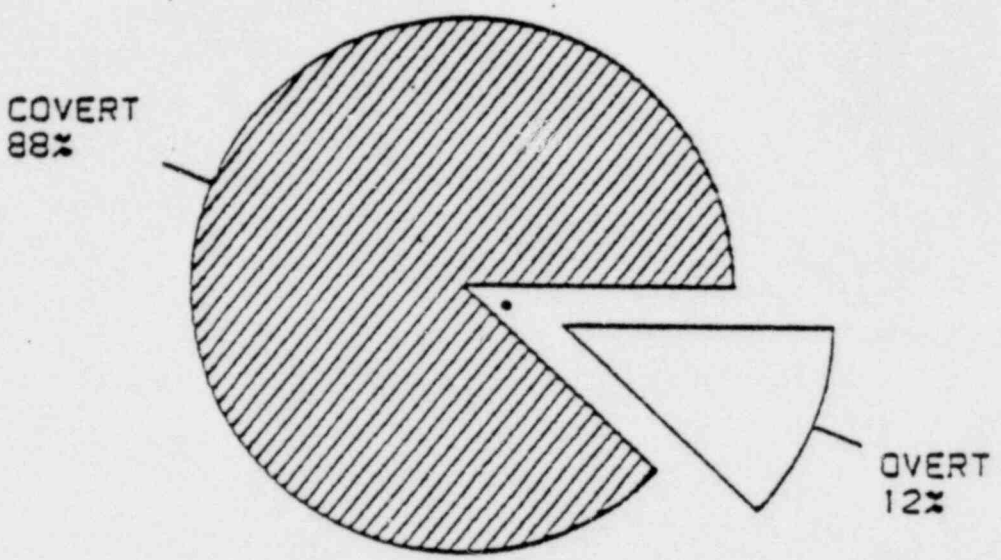


FIGURE G.24

DISTRIBUTION OF TYPES OF ROLE: SABOTAGE*



*TOTAL NUMBER OF DATA POINTS FOR THIS CHARACTERISTIC WAS 33. INCLUDES ANALOGS 1&2 AND SPECIAL CASES.

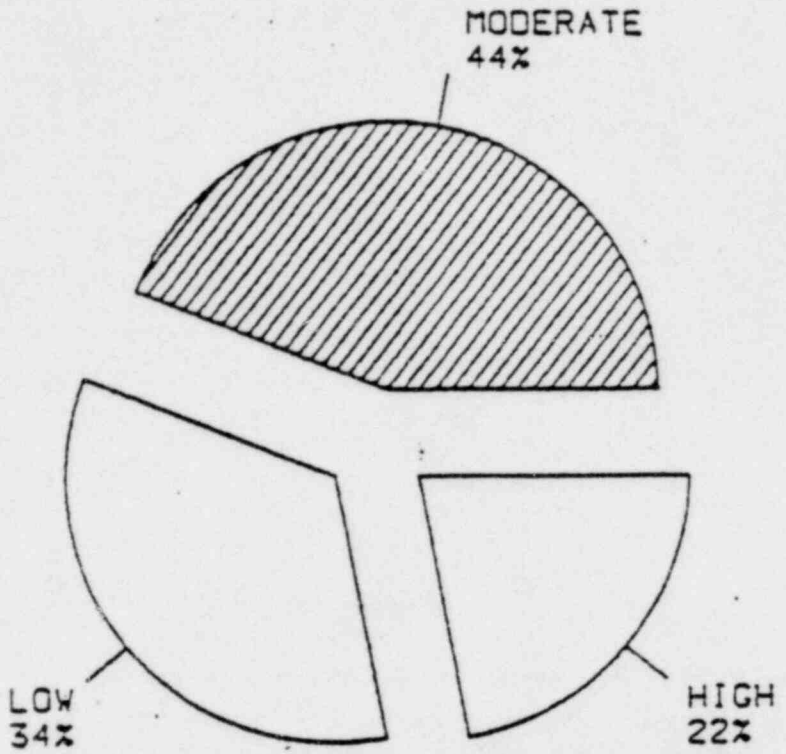
The following definitions were used:

1. Overt - the insider was able to perpetrate the crime in the presence of others without arousing suspicion

2. Covert - the insider was unable to perpetrate the crime in the presence of others without arousing suspicion

FIGURE G.25

DISTRIBUTION OF LEVELS OF PLANNING: SABOTAGE*



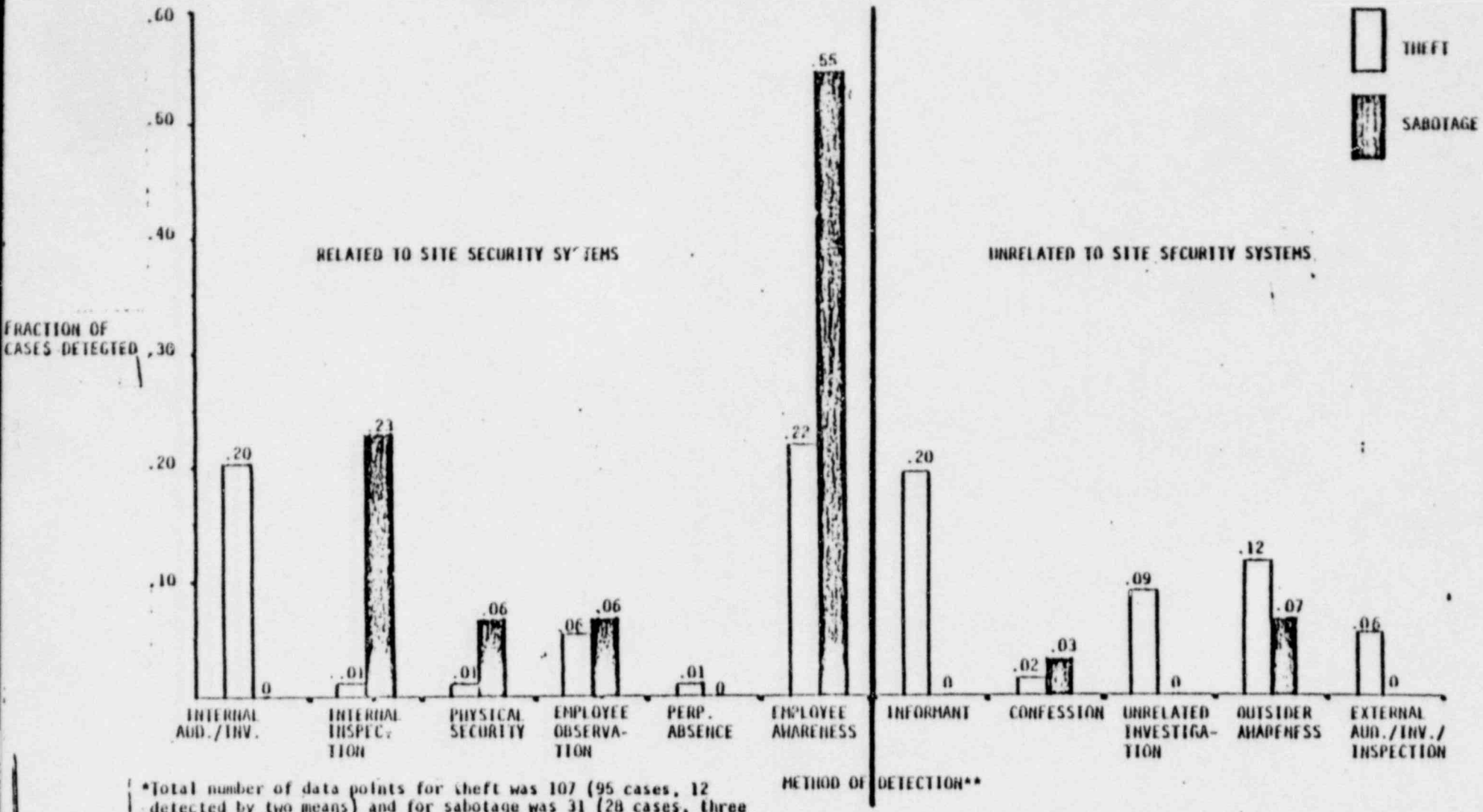
*TOTAL NUMBER OF DATA POINTS FOR THIS CHARACTERISTIC WAS 32. INCLUDES ANALOGS 1&2 AND SPECIAL CASES.

The following definitions were used:

1. High - the insider planned the crime thoroughly and precisely
2. Moderate - the insider planned the crime, but with less attention to detail
3. Low - very little planning was revealed; the crime may have been a spur of the moment act executed against a target of opportunity

Figure 5.26

COMPARISON OF DISTRIBUTION [illegible]THOD OF DETECTION:
THEFT (ANALOG 1 AND 2) AND SABOTAGE (ANALOG 1 AND 2 AND SPECIAL CASES)*



*Total number of data points for theft was 107 (95 cases, 12 detected by two means) and for sabotage was 31 (28 cases, three detected by two means).
**For definitions, see pp. 5-5 and 5-6.

Table G.1

DISTRIBUTION OF MOST FREQUENT MOTIVATIONS BY TARGET CONTROL TYPE: THEFT, ANALOGS 1 & 2*

MOTIVATION	POLICYMAKER/MANAGER	OPERATIONAL	NONE
	Motivation Distribution %		
Greed	68	61	71
Financial Inducement	8	14	0
Drug Abuse	1	7	9
Peer Pressure	8	0	4
Personal Loyalty	3	6	4
Disgruntlement	1	1	4
Psychological	0	0	4
Indebtedness	3	2	0
Other	8	9	4
Total	100	100	100
*No. of Data Points=	65	224	24

The following definitions were used:

1. Policy/Manager - the insider is responsible for determining (controlling) or implementing organizational or procedural policy at the targeted activity or site.

2. Operational - the insider is a non-supervisory line/operations functionary whose routine job duties bring him into contact with the target.

3. None - the insider exercised no control over the target.

Table G.2

DISTRIBUTION OF TYPES OF ACCESS BY TARGET CONTROL
TYPE: THEFT, ANALOGS 1 & 2*

TYPES OF ACCESS	POLICYMAKER/MANAGER	OPERATIONAL	NONE
		Access Distribution %	
Routine	80	94	17
Non-Routine	20	6	83
Total	100	100	100
*No. of Data Points=	50	162	23

The following definitions were used:

1. Routine access - the insider used his normal, authorized access to the target to perpetrate the crime.

2. Non-routine access - the insider circumvented or violated some type of access control or gained access to a target that was not part of his normal job duties or routine.

Table G.3

DISTRIBUTION OF TYPES OF ROLE BY TARGET CONTROL
TYPE: THEFT, ANALOGS 1 & 2*

TYPE OF ROLE	POLICYMAKER/MANAGER	OPERATIONAL	NONE
		Role Distribution %	
Overt	38	37	0
Covert	62	63	100
Total	100	100	100
*No.of Data Points=	50	162	23

The following definitions were used:

1. Covert - the insider was unable to perpetrate the crime in the presence of others without arousing their suspicion.

2. Overt - the insider was able to perpetrate the crime in the presence of others without arousing suspicion.

Table G.4

DISTRIBUTION OF TYPES OF STIMULI BY TARGET CONTROL TYPE: THEFT, ANALOGS 1 & 2*

STIMULUS	POLICYMAKER/MANAGER	OPERATIONAL	NONE
		Stimuli Distribution %	
Self-initiated	87	74	100
Induced Internal	2	11	0
Induced External	9	11	0
Unwitting	2	4	0
Total	100	100	100
*No of Data Points=	51	168	26

The following definitions were used:

1. Self-initiated - the insider participated in the crime at his own initiation.

2. Levered by insider - the insider was persuaded by some inducement or threat offered or made by another insider to participate in the crime.

3. Levered by outsider - the insider was persuaded by some inducement or threat offered or made by someone external to the targeted facility or activity to participate in the crime.

4. Unwitting - the insider contributed in some way to the commission of the crime, but was unaware of his involvement in a criminal activity.

Table G.5

DISTRIBUTION OF LEVEL OF PLANNING BY TARGET CONTROL TYPE: THEFT, ANALOGS 1 & 2*

LEVEL OF PLANNING	POLICYMAKER/MANAGER	OPERATIONAL	NONE
	Planning Level Distribution %		
Low	10	14	35
Moderate	18	42	61
High	72	44	4
Total	100	100	100
*No. of Data Points-	48	153	23

The following definitions were used:

1. High - the insider planned the crime thoroughly and precisely.
2. Moderate - the insider planned for the crime, but with less attention to detail.
3. Low - very little planning was revealed; the crime may have been a spur of the moment act executed against a target of opportunity.

Table G.6

DISTRIBUTION OF DEGRESS OF OUTSIDE INVOLVEMENT BY TARGET CONTROL TYPE: THEFT, ANALOGS 1 & 2*

OUTSIDE GROUP SIZE	POLICYMAKER/MANAGER	OPERATIONAL	NONE
	Group Size Distribution %		
1	16	12	17
More than 1	20	25	35
None	64	63	48
Total	100	100	100
*No. of Data Points-	50	162	23

External involvement means that a person(s) not formally associated with the targeted facility participated in the crime in some way.

Table G.7

DISTRIBUTION OF TACTICS BY TARGET CONTROL
TYPE: THEFT, ANALOGS 1 & 2*

TACTIC	POLICYMAKER/MANAGER	OPERATIONAL	NONE
	Tactics Distribution %		
Falsified Documents	20	6	0
Slush Funds/Laundered Money	5	1	0
Disabling Alarms	0	1	8
False Identification	0	1	8
Misrepresentation of Self/ Authority	0	4	8
Ransom/Extortion	0	0	8
Phony Documents	6	4	0
Abuse of Trust	17	8	0
Surreptitious Removal	15	42	50
Guile, Ruse, Deceit	11	9	17
Other	26	24	1
Total	100	100	100
*No. of Data Points=	66	106	12

Table G.8

DISTRIBUTION OF TACTICS INVOLVING MANIPULATION OF PROCEDURES AND RESOURCES BY TARGET CONTROL TYPE: THEFT, ANALOGS 1 & 2*

TACTIC	POLICYMAKER/MANAGER	OPERATIONAL	NONE
		Tactics Distribution %	
Falsified Documents	20	7	0
Computer Manipulation	6	5	0
Phony Documents	6	5	0
Slush Funds	4	0	0
Destruction of Records	3	2	0
Price Fixing	2	0	0
Forgery	3	2	0
All Tactics Used, %	44	21	0
*No. of Data Points=	29	17	0

Table G.9

DISTRIBUTION OF TACTICS INVOLVING SUBTERFUGE BY TARGET CONTROL TYPE: THEFT, ANALOGS 1 & 2*

TACTIC	POLICYMAKER/MANAGER	OPERATION	NONE
		Tactics Distribution %	
Surreptitious Removal	15	42	50
Guile, Ruse, Deceit	11	9	17
Misrepresentation of Self, Authority	0	4	8
False I/D	0	1	8
Infiltration	0	2	0
All Tactics Used, %	26	58	83
*No. of Data Points=	17	61	10

Table G.10

DISTRIBUTION OF MOTIVATIONS: THEFT, ANALOG 1 AND 2 COMPARISON*

MOTIVATION	Analog 1 Insiders, %	Analog 2 Insiders, %
	Motivations Distribution %	
Greed	55	75
Financial Inducement	15	7
Personal Loyalty	8	2
Drug Use	5	7
Blackmail	2	0
Threats	2	1
Debt	2	2
Peer Pressure	2	2
Disgruntlement	2	1
Power Play	2	0
Other**	5	3
TOTAL	100	100

*Total number of data points for this characteristic was 311.
**For the complete list of motivations, see Table G.11.

Table G.11

COMPLETE DISTRIBUTION OF MOTIVATIONS:
THEFT, ANALOG 1 AND 2 COMPARISON*

MOTIVATION	ANALOG 1 INSIDERS, %	ANALOG 2 INSIDERS, %
	Motivation Distribution %	
Greed	54	75
Revenge	1	0
Disgruntlement	2	1
Company Loyalty	0	0
Personal Loyalty	8	2
Blackmail	3	0
Desire for Recognition	0	0
Power Play	2	0
Threat	3	1
Psychological/Personal Problems	0	1
Game Playing	2	0
Ideology	0	0
Demonstrate Security Laxity	0	7
Indebtedness	2	2
Gambling	0	1
Drug Abuse	5	7
Sex	1	0
Marital Problems	0	1
Peer Pressure	2	2
Financial Inducement	15	7

*Total number of data points for this characteristic was 311.

Table G.12

DISTRIBUTION OF TACTICS: THEFT, ANALOG 1 AND 2 COMPARISON*

TACTIC USED**	Analog 1 Cases, %	Analog 2 Cases, %
	Tactics Distribution %	
Surreptitious Removal	24	48
Altered or Falsified Documentation	16	6
Guile, Ruse, Deceit	10	15
Abuse of Trust	11	9
Illicit Sales	9	2
Phony Documents or Company	7	2
Computer Manipulation	7	2
Other**	16	16
TOTAL	100	100

*Total number of data points for this characteristic was 265 (179 for analog 1 and 86 for analog 2).
**For the complete list of tactics, see Table G.13.

Table G.13

COMPLETE DISTRIBUTION OF TACTICS:
THEFT, ANALOG 1 AND 2 COMPARISON*

TACTIC	ANALOG 1 INSIDERS, %	ANALOG 2 INSIDERS, %
	Tactics Distribution %	
Computer Manipulation	7	1
Falsified Documents/ Document Manipulation	16	6
Guile, Ruse, Deceit	10	15
Abuse of Trust	11	9
Surreptitious Removal	23	48
Illicit Sales	9	2
Misrepresentation of Self, Authority, Position	3	4
Arson	0	1
Disable Target	0	0
Hijacking	1	0
Explosion	0	0
Price Fixing	1	0
False Identification	1	1
Illicit Transfer of Knowledge	1	1
False Advertising	0	0
Concealment/Destruction of Information/Records	4	1
Forgery	2	0
Slush Funds	2	0
Phony Documents, Accounts, Invoices, Companies	7	2
Surreptitious Entry/Exit	1	2
Foreign Objects Used in Sabotage	0	0
Disabling Alarms	0	2
Ransom/Extortion	0	1
Infiltration	1	2

*Total number of data points for this characteristic was 265.

Table G.14

COMPLETE DISTRIBUTION OF MOTIVATIONS:
SABOTAGE (ANALOG 1, 2 AND SPECIAL CASES)*

MOTIVATION	INSIDE SABOTEURS, %
Greed	8
Revenge	17
Disgruntlement	17
Company Loyalty	4
Personal Loyalty	2
Blackmail	0
Desire for Recognition	8
Power Play	0
Threat	2
Psychological/Personal Problems	17
Game Playing	0
Ideology	8
Demonstrate Security Laxity	4
Indebtedness	2
Gambling	0
Drug Abuse	6
Sex	0
Marital Problems	0
Peer Pressure	4
Financial Inducement	0

*Total number of data points for this characteristic was 51.

Table G.15

DISTRIBUTION OF TACTICS:
SABOTAGE (ANALOG 1, 2 AND SPECIAL CASES)*

TACTIC	INSIDE SABOTEURS, %
Computer Manipulation	0
Falsified Documents/ Document Manipulation	0
Guile, Ruse, Deceit	6
Abuse of Trust	4
Surreptitious Removal	4
Illicit Sales	0
Misrepresentation of Self, Authority, Position	2
Arson	13
Disabling Target	40
Hijacking	0
Explosion	4
Price Fixing	0
False Identification	0
Illicit Transfer of Knowledge	0
False Advertising	0
Concealment/Destruction of Information/Records	4
Forgery	0
Slush Funds	0
Phony Documents, Accounts, Invoices, Companies	0
Surreptitious Entry/Exit	11
Foreign Objects Used in Sabotage	10
Disabling Alarms	2
Ransom/Extortion	0
Infiltration	0

*Total number of data points for this characteristic was 52.

Table G.16

Distribution of Method of Detection: Theft, Analog 1*

Method of Detection**	Frac. of Cases Detected
Related to Site Security Systems	
Internal Audit/Inventory	.13
Internal Inspection	.02
Physical Security	.02
Employee Observation	.03
Perpetrator Absence	.02
Employee Awareness of Abnormal Activity/Condition	.21
	.43
Unrelated to Site Security Systems	
Informant	.21
Confession	.03
Investigation of Unrelated Activity	.13
Outsider Awareness of Abnormal Activity/Condition	.14
External Audit/Inventory/ Inspection	.06
	.57

*Total number of cases with data on this variable is 57. In five cases, the crime was detected by two means, yielding 62 detections.

**For definitions, see pp. 5-5 and 5-6.

Table G.17

Distribution of Method of Detection: Theft, Analog 2*

Method of Detection**	Frac. of Cases Detected
Related to Site Security Systems	
Internal Audit/Inventory	.31
Internal Inspection	0
Physical Security	0
Employee Observation	.09
Perpetrator Absence	0
Employee Awareness of Abnormal Activity/Condition	.25
	.65
Unrelated to Site Security Systems	
Informant	.18
Confession	0
Investigation of Unrelated Activity	.04
Outsider Awareness of Abnormal Activity/Condition	.09
External Audit/Inventory/ Inspection	.04
	.35

*Total number of cases with data on this variable is 43. In two cases, the crime was detected by two means, yielding 45 detections.

**For definitions, see pp. 5-5 and 5-6.

Table G.18

Distribution of Method of Detection Conditional upon Target Control of Insiders: Theft (Analogs 1 and 2) vs. Sabotage (Analogs 1 and 2 and Special Cases)*

Method of Detection**

Related to Site Security Systems

	given that TARGET CONTROL is:	INTER. AUDIT/ INVEN.	INTER. INSP.	PHYS. SEC.	EMPL. OBSER.	PERP. ABSENCE	EMPL. AWARENESS	TOTAL
	Pol./Mgt.	.30	0	0	.01	0	.16	.47
THEFT	Operational	.24	.01	.01	.02	.01	.17	.46
	None	.34	0	0	.04	0	.08	.46
	Pol./Mgt.	0	0	.16	.17	0	.50	.83
SABOTAGE	Operational	0	.24	.05	0	0	.62	.91
	None	0	.30	0	.10	0	.60	1.00

Unrelated to Site Security Systems

	given that TARGET CONTROL is:	INFOR-MANT	CON-FESSION	UNRELATED INVESTI-GATION	OUTSIDER AWARENESS	EXT. AUDIT/ INVEN./ INSP.	TOTAL
	Pol./Mgt.	.16	.04	.13	.15	.05	.53
THEFT	Operational	.21	.05	.03	.19	.06	.54
	None	.31	0	.08	0	.15	.54
	Pol./Mgt.	0	0	0	.17	0	.17
SABOTAGE	Operational	0	.05	0	0	.04	.09
	None	0	0	0	0	0	0

*Total number of data points was 223 for theft and 37 for sabotage.

**For definitions, see pp. 5-5 and 5-6

Table G.19

Distribution of Method of Detection Conditional upon Role of Insider: Theft, Analogs 1 and 2*

Method of Detection**

Related to Site Security Systems

		INTER. AUDIT/ INVEN.	INTER. INSP.	PHYS. SEC.	EMPL. OBSER.	PERP. ABSENCE	EMPL. AWARENESS	TOTAL
given that ROLE of Insider is	OVERT	.34	0	0	.03	.01	.16	.54
	COVERT	.21	.01	.01	.02	0	.19	.44

Unrelated to Site Security Systems

		INFOR-MANT	CON-FESSION	UNRELATED INVESTI-GATION	OUTSIDER AWARENESS	EXT. AUDIT/ INVEN./ INSP.	TOTAL
given that ROLE of Insider is	OVERT	.21	.05	.07	.05	.08	.46
	COVERT	.20	.04	.03	.20	.09	.56

*Total number of insiders with data on this variable was 223 (75 overt and 148 covert).

**For definitions, see pp. 5-5 and 5-6.

Table G.20

Distribution of Method of Detection Conditional upon Number of Insiders: Theft (Analogs 1 and 2) vs Sabotage (Analogs 1 and 2, and Special Cases)*

Method of Detection**

Related to Site Security Systems

	given that INSIDER GROUP SIZE is:	INTER. AUDIT/ INVEN.	INTER. INSP.	PHYS. SEC	EMPL. OBSER	PERP. ABSENCE	EMPL. AWARENESS	TOTAL
THEFT	1	.26	0	0	.09	.02	.28	.65
	2 or > 2	.32	0	0	0	0	.21	.53
SABOTAGE	1	0	.26	.09	.09	0	.52	.96
	2 or > 2	0	.25	0	0	0	.50	.75

Unrelated to Site Security Systems

	given that INSIDER GROUP SIZE is:	INFOR-MANT	CON-FESSION	UNRELATED INVESTI-GATION	OUTSIDER AWARENESS	EXT. AUDIT/ INVEN./ INSP.	TOTAL
THEFT	1	.17	0	.07	.09	.02	.35
	2 or > 2	.16	.05	0	.16	.10	.47
SABOTAGE	1	0	.04	0	0	0	.04
	2 or > 2	0	0	0	.25	0	.25

* Total number of data points was 62 for theft (43 of a single insider and 19 of two or more insiders) and 27 for sabotage (23 single and 4 two or more). Excludes cases that involved outsider collusion.

** For definitions, see pp. 5-5 and 5-6.

Table G.21

Distribution of Method of Detection Conditional upon Insider/Outsider Conspiracy: Theft, Analogs 1 and 2*

Method of Detection**

Related to Site Security Systems

Given INSIDER/OUTSIDER Conspiracy	INTER. AUDIT/ INVEN.	INTER. INSP.	PHYS. SEC.	EMPL. OBSER.	PERP. ABSENCE	EMPL. AWARENESS	TOTAL
	.11	.02	.03	.06	0	.18	.40

Unrelated to Site Security Systems

Given INSIDER/OUTSIDER Conspiracy	INFOR-MANT	CON-FESSION	UNRELATED INVESTI-GATION	OUTSIDER AWARENESS	EXT. AUDIT/ INVEN./ INSP.	TOTAL
	.22	.02	.16	.13	.07	.60

* Total number of cases with data on this variable was 42. In three cases, the conspiracy was detected by two means, yielding 45 data points.

** For definitions, see pp. 5-5 and 5-6.

Table G.22

DISTRIBUTION OF INSIDER GROUP SIZE CONDITIONAL UPON LEVEL OF SCREENING: THEFT, ANALOGS 1 AND 2*

Given that LEVEL OF SCREENING** is:	INSIDER GROUP SIZE	
	1	2 or >2
Good	.61	.39
Fair	.37	.63
Poor	.30	.70
None	.33	.67

*Total number of data points for these characteristics was 169 (63 single insiders and 106 insiders in conspiracy with other insiders). For any given conspiracy, the perpetrators may not have undergone the same level of screening.

**For definitions, see Figure G.3.

Table G.23

DISTRIBUTION OF INSIDER GROUP SIZE CONDITIONAL UPON LEVEL OF SCREENING: SABOTAGE, ANALOGS 1 AND 2 AND SPECIAL CASES*

Given that LEVEL OF SCREENING** is:	INSIDER GROUP SIZE	
	1	2 or >2
Good	.77	.23
Fair	.33	.67
Poor	.50	.50
None	1.00	0

*Total number of data points for these characteristics was 34 (16 single insiders and 12 insiders in conspiracy with other insiders).

**For definitions, see Figure G.3.

Table G.24

DISTRIBUTION OF LENGTH OF SERVICE CONDITIONAL UPON LEVEL OF SCREENING: THEFT, ANALOGS 1 AND 2*

Given that LEVEL OF SCREENING** IS	LENGTH OF SERVICE			
	0-5 yrs.	6-10 yrs.	11-15 yrs.	>15 yrs.
Good	.38	.39	.15	.08
Fair	.39	.53	.04	.04
Poor	.50	.33	.13	.04
None	.69	.19	.06	.06

*Total number of data points for these characteristics was 107.

**For definitions, see Figure G.3.

Table G.25

COMPARISON OF PRP DISQUALIFICATION CAUSES*

January 1 - December 31, 1978

Component	PRP Positions	1. Alcohol	2. Marijuana and Other Drugs	3. Negligence/ Delinquency	4. Court-Martial/ Civil Convictions	5. Behavior/Contemptuous Attitude/Physical/ Mental	6. Poor Attitude/ Motivation	Total 1-6	%
Army	22,666	142	703	31	152	327	111	1,466	6.47
Navy	39,098	107	623	135	253	325	203	1,646	4.21
Air Force	53,967	129	642	335	352	714	508	2,680	4.97
JCS	155	0	0	0	0	0	0	0	0
NSA	337	0	4	0	0	1	0	5	1.48
DNA	30	0	0	0	0	0	0	0	0
TOTAL	116,253	378	1,972	501	757	1,367	822	5,797	4.99
U.S.	87,330	222	1,153	396	537	955	603	3,866	4.43
Pacific	5,830	13	55	18	22	76	25	209	3.58
Europe	23,093	143	764	87	198	336	194	1,722	7.46

*Source: DOD Office of Security Policy.

APPENDIX H

BIBLIOGRAPHY

Bequai, August. "Analysis of Insider Related Threats." Washington, prepared under contract to USNRC, 1979.

Bequai, August. White-Collar Crime: A 20th Century Crisis. Lexington, MA: D.C. Heath and Company, 1978.

Bickwit, Leonard Jr. Memorandum on NRC Clearance Rule Proceeding: OGC Comments. Washington: U.S. Nuclear Regulatory Commission, July 30, 1979.

Brittell, Frank. "Survey of the Insider Threat to the Nuclear Industry." Los Angeles, prepared under contract to USNRC, 1979.

Clark, John P.; Holinger, Richard C.; and Smith, Leonard F. Theft by Employees in Work Organizations - A Preliminary Final Report. Minneapolis: University of Minnesota Department of Sociology (prepared under grant from U.S. Department of Justice), 1979.

Edelhertz, Herbert, and Walsh, Marilyn. The White-Collar Challenge to Nuclear Safeguards. Lexington, MA: D.C. Heath and Company (prepared under contract to USNRC), 1978.

Fraud Bulletin No. 60. Park Ridge, IL: Bank Adminisration Institute, 1977.

Heineke, John M. The Insider Threat to Secure Facilities: Data Analysis. Livermore, CA: Lawrence Livermore Laboratory (prepared under contract to USNRC), 1979.

Kull, L.; Harris, L.; and Lobner, P. Protection of Nuclear Power Plants against Sabotage by An Insider. La Jolla, CA: Science Applications, Inc. (prepared under contract to Brookhaven National Laboratory), 1978.

Kull, L.; Harris, L.; Lobner, P.; and El-Bassioni, A. Protection of Nuclear Power Plants against Sabotage by Two Insiders. La Jolla, CA: Science Applications, Inc. (prepared under contract to Brookhaven National Laboratory), 1978.

Leachman, Robert, and Althoff, Phillip, eds. Preventing Nuclear Theft: Guidelines for Industry and Government. New York: Praeger, 1972.

McDaniel, T. L.; Glancy, J. E.; and Horton, W. H. Safeguards against Insider Collusion. Washington: U.S. Nuclear Regulatory Commission, NUREG/CR-0532, vol. 1 (prepared under contract by Science Applications, Inc.), 1979.

Minogue, Robert B. Commission Paper on Proposed Amendment to 10 CFR Part 73.55 to Extend the Implementation Date for Certain Complementary and Alternative Measures for Protection against the Insider Threat. Washington: U.S. Nuclear Regulatory Commission, SECY 79-59, January 24, 1979.

Parker, Donn B. Computer Abuse Assessment. Menlo Park, CA: Stanford Research Institute, 1975.

Parker, Donn B. Crime by Computer. New York: Charles Scribner's Sons, 1976.

Perry, Ronald W.; Bennett, Carl A.; and Wood, Michael T. The Role of Security Clearances and Personnel Reliability Programs in Protecting against Insider Threats. Seattle: Battelle Human Affairs Research Centers (prepared under contract to Sandia Laboratory), 1979.

Schechter, Richard. The Insider Threat to Secure Facilities - A Synopsis of Nine Interviews. Washington: U.S. Nuclear Regulatory Commission, NUREG/CR-1279 (prepared under contract by Lawrence Livermore Laboratory), 1980.

Shapar, Howard K. Memorandum on Clearance Rule Proceedings. Washington: U.S. Nuclear Regulatory Commission, July 16, 1979.

Shapar, Howard K. Memorandum on SECY 79-319, Response to Commission Requests in Clearance Rule Proceeding. Washington: U.S. Nuclear Regulatory Commission, July 31, 1979.

A Study to Assess the Radiological Sabotage Potential of Operating Nuclear Power Plants. Washington: KMC, Inc., 1978.

Sutton, Richard Jr. "Insider Threat Survey of Analogous Private Industries." Washington, prepared under contract to USNRC, 1979.

U.S. Comptroller General. Report to the Congress: Automated Systems Security--Federal Agencies Should Strengthen Safeguards over Personal and Other Sensitive Data. Washington: U.S. General Accounting Office, 1979.

U.S. Department of the Army. Nuclear and Chemical Weapons and Materiel: Chemical Surety Program. Washington: USDOA Regulation No. 50-6, 1978.

U.S. Department of the Army. Nuclear and Chemical Weapons and Materiel: Nuclear Surety. Washington: USDOA Regulation No. 50-5, 1978.

U.S. Department of the Army. Subversion and Espionage Directed against the U.S. Army. Fort Huachuca, AZ: USDOA Intelligence Center and School, 1975.

U.S. Department of Defense. Nuclear Weapon Personnel Reliability Program. Washington: USDOD Directive No. 5210.42, 1978.

U.S. Department of Energy. "Department of Energy Nuclear Weapon Safety Program (Draft)." Washington: USDOE Order No. 5620.1, 1979. (Mimeographed.)

U.S. Department of Transportation. Guidelines for the Physical Security of Cargo. Washington: USDOT, Office of the Secretary, 1979.

U.S. Federal Personnel Manual, Chapter 736, "Investigations." Washington: Government Printing Office. 1978.

U.S. National Bureau of Standards and Defense Nuclear Agency. Proceedings of the Second Annual Symposium, March 23-24, 1977: The Role of Behavioral Science in Physical Security. Washington: Government Printing Office, 1978.

U.S. Nuclear Regulatory Commission. "Behavioral Observation Program to Assure Continued Reliability of Employees". Washington: USNRC Contract No. 01-79-003, 1979.

U.S. Nuclear Regulatory Commission. "Report of the Hearing Board in the Matter of Authorization for Access to or Control over Special Nuclear Material." Washington: USNRC Docket No. RM 50-7, April 5, 1979.

U.S. Nuclear Regulatory Commission. Report of the Material Control and Material Accounting Task Force. Washington: USNRC, NUREG-0450 vol. 3, 1978.

U.S. Nuclear Regulatory Commission. "Staff's Concluding Statement in the Matter of Special Nuclear Material, Auth[illegible] for Access to or Control." Washington: USNRC Docket No. RM 50-7, Septem[illegible]78.

U.S. Nuclear Regulatory Commission. "Standards for Psychological Assessment of Security Personnel." Washington: USNRC Contract No. 01-79-002, 1979. (Amended to cover all nuclear industry personnel.)

U.S. Nuclear Regulatory Commission. "Written Testimony of NRC Staff Re: Authority for Access to or Control over Special Nuclear Material." USNRC Docket No. RM 50-7, July, 1978.