# Insider Crime

## The Threat to Nuclear Facilities and Programs

Bruce Hoffman, Christina Meyer,
Benjamin Schwarz, Jennifer Duncan

The research described in this report was sponsored by the U.S. Department of Energy.

ISBN: 0-8330-0983-4



Published by The RAND Corporation
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90406-2138

R-3782-DOE

# Insider Crime

## The Threat to Nuclear Facilities and Programs

Bruce Hoffman, Christina Meyer,
Benjamin Schwarz, Jennifer Duncan

February 1990

Prepared for the
U.S. Department of Energy

RAND

# PREFACE

This report presents the results of a study sponsored jointly by the Office of Threat Assessment, Department of Energy (DOE), and Sandia National Laboratories. The study was undertaken to gain insight into the threat posed by hostile employees, or "insiders," to DOE nuclear programs.

By examining the historical data on 62 reported insider crimes, this report explores some of the characteristics of potential criminal actions against nuclear facilities or programs that might be executed by, or with the assistance of, insiders.

The work was carried out in the International Security and Defense Policy Program of the National Security Research Division at RAND, under a project entitled "The Threat Posed by Insiders to DOE Nuclear Programs."

# SUMMARY

This report explores the characteristics of 62 reported "insider" crimes that may provide insights into potential threats to the security of Department of Energy (DOE) nuclear weapons programs. There have been few actual criminal incidents against nuclear facilities, so threat assessments must rely on analogs. These 62 conventional crimes were selected for study because their aims and operations are similar to those of possible future crimes involving nuclear weapons facilities or nuclear material.

Insider crime in general, and especially crime that involves thefts of great value or that poses substantial risks to the perpetrator, is arguably one of the least understood areas of criminology. To gain a better understanding of these incidents and of how insiders might pose a threat to DOE nuclear programs, this study attempts to identify characteristics of potential criminal nuclear actions that might be executed by, or with the assistance of, insiders. In particular, it considers:

- The identity of the insider, including his or her motivations, age, length of employment, and status within the corporation, institution, or government agency.
- The particulars of the crime, including the illegal action perpetrated and, in the case of theft, what was taken; how the insider gained access to the target; and how he or she was persuaded to commit the crime.
- The effectiveness of the security procedures of the corporation, institution, or agency, specifically those implemented to prevent insider crime, and any changes in those procedures that might have resulted from these crimes.

We organized the types of insider crime into three categories:

- Crimes committed by insiders conspiring with outsiders.
- Crimes committed by insiders conspiring with other insiders.
- Crimes committed by lone insiders.

The first type we deemed most analogous to potential attacks on nuclear facilities, because terrorists or foreign agents—or even professional criminals—with access to the help of an insider would seem more likely to attempt such crimes than would a group of insiders or an insider working alone. Nevertheless, we examined the single insider

to obtain further information on the characteristics of insiders, and the insider conspiracy group to learn more about both insiders and the nature of conspiracies.

Crimes committed by insiders and outsiders working together display more of the characteristics associated with a hypothetical nuclear crime than do those committed by the other two groups. Specifically, the insider/outsider crimes considered in this study involved well-laid plans and associates who had sought, or had been sought by, insiders. We must emphasize that the threat posed by multiple insiders or a lone insider is not negligible. An insider driven by a psychological or emotional disturbance could steal nuclear material or cause significant destruction to a nuclear facility. By the same token, a conspiratorial group of insiders could steal nuclear material, with the intention of finding a buyer or undertaking some blackmail scheme.

Insiders in all three categories committed most of their crimes for financial gain. Even in the two incidents that actually involved terrorist groups (the robbery of an armored car by members of the Order and the robbery of an armored car depot by *Los Macheteros*) and the one that involved a foreign government (the theft of weapons from the Naval aviation depot that were subsequently sold to Iran), insiders assisted not only for reasons of ideological affinity or sympathy, but also because of promised monetary reward. These examples suggest that a terrorist group could secure an insider's assistance simply by paying him or her.

The greatest number of crimes committed for other than financial gain were committed by lone insiders. These individuals, on the whole, appeared to be less stable than the others. One-third of them were motivated by emotional disturbance, frustration with their employment, or idiosyncratic factors.

Perhaps the most important finding of this study relates to planning and security. Success in most of the incidents examined seemed to depend less on detailed planning or expert execution than on the exploitation of existing security flaws. Indeed, most of these crimes did not require sophisticated planning; they were carried out against targets of opportunity. Even those companies that were heavily secured were robbed or burgled by insiders using routine access to exploit situations where security was lax. However, it should be emphasized that none of the organizations in our database employed security equivalent to that at a nuclear facility.

Guard forces present a special and particularly vexing problem. Guards were responsible for 41 percent of the crimes committed *against guarded targets.* In many cases, the security routines themselves appeared to be adequate, but they were not properly followed. This

problem could be alleviated by providing guards with some positive motivation such as rotation from monotonous routines, or higher pay to instill a sense of long-term commitment to their jobs and employers.

In sum, insider criminals may be among the most difficult and dangerous adversaries to defend against. They may be young or old, long-time or short-time employees. Although financial gain may be the insider's predominant motivation, family ties, intimate relationships, disillusionment or disgruntlement, misplaced altruism, and ideological allegiances may also play a role in the decision to commit or abet a criminal act against an employer. Insiders can accomplish great damage acting either alone, in cooperation with fellow insiders, or in league with outsiders.

Beyond a certain point, security considerations in hiring, guarding, controlling, and checking people can become so cumbersome as to impede the operation of the facility they are meant to protect. Therefore, no organization, no matter how ingeniously protected, can operate without some trust in individuals on all levels. This illuminates the problem inherent in all situations involving nuclear material: One accident or one successful crime is one too many. If a bank is robbed, or jewels are stolen, or a factory is sabotaged or vandalized, society at large generally does not suffer major disruption or discomfiture. But the social and political—as well, obviously, as the physical—fallout from a nuclear crime is such that adequate, or even very good, protection is not enough. Total security can never be attained, nor can insider crime ever be completely prevented. However, security officials can and must keep all possibilities in mind at all times, to avoid surprises and to be prepared at least to minimize damage.

# ACKNOWLEDGMENTS

The research reported here would not have been possible without the assistance of Orli Peter and Rachel Kaganoff. Konrad Kellen and Carl Builder provided extraordinarily incisive and helpful technical reviews of the manuscript, and Tom Blankenship, Ben Bader, and David McVey offered the authors sound advice throughout the project. A particular debt is owed to the numerous corporate officers, security directors, law enforcement personnel, and threat analysts who were interviewed in the course of our research but who prefer to remain anonymous. Finally, Janet DeLand's editorial skills greatly improved a difficult manuscript.

# CONTENTS

# TABLES

# I. INTRODUCTION

This report explores the characteristics of 62 crimes that may provide analogs to potential threats to the security of Department of Energy (DOE) nuclear weapons programs. Officials responsible for the security of these programs must anticipate a wide variety of threats from an array of potential adversaries with ideological, economic, or personal motivations. However, it is very difficult to assess these threats because of the lack of empirical data. There have been few actual criminal incidents against nuclear facilities. However, the conventional crimes examined in this study are similar in their aims and operations to possible future crimes involving nuclear weapons facilities or nuclear material. Study of these crimes may therefore provide insights into the capabilities and modus operandi of potential adversaries to nuclear programs; evidence about the methods that might be used in theft, sabotage, or extortion; and information about the effectiveness of various kinds of security procedures in preventing potential nuclear crimes.

The theft of strategic nuclear material is most likely to be attempted by either anti-nuclear groups, psychotics, criminals, terrorists, or foreign agents. Of these, anti-nuclear groups, psychotics, and criminals probably present the least danger. Although anti-nuclear groups might stage violent demonstrations, they are ideologically averse to causing death or destruction with nuclear material. Psychotics, with their irrational reasoning, pose a frightening and unpredictable threat, but they would probably have difficulty convincing others to support them in a dangerous scheme. And working alone, they would have trouble penetrating the security systems of a nuclear facility. Criminals, motivated by economic gain, would be less attracted to stealing strategic nuclear material than other, less risky and more easily marketable commodities. Strategic nuclear material would be most valuable to those intending to use it for political reasons, in particular, terrorists and agents working for foreign governments. Of course, these groups may decide to use criminals or psychotics to help them carry out their schemes.

Given the problems that any of these groups would face in attempting to steal strategic nuclear material from a DOE weapons facility, such crimes would require detailed and intimate knowledge of the facility's security programs, procedures, operations, physical layout, and, of course, the location of the material targeted for theft. The

most likely source of such information would be an employee of the facility, an "insider" who might be coerced or convinced to help, or who might actually suggest the crime. This study focuses on the possible roles such an insider might play in a potential nuclear crime.

Insider crime, in general, and especially crime that involves thefts of great value or that poses substantial risks to the perpetrator, is one of the least understood areas of criminology.[1] To better understand such incidents and to gain insight into how insiders might pose a threat to DOE nuclear programs, we have examined historical data on 62 reported insider crimes.[2] We focus on three aspects of the crimes:

- The identity of the insider, including his or her motivations, age, length of employment, and status within the corporation, institution, or government agency.
- The particulars of the crime, including the illegal action the insider perpetrated and, in the case of theft, what was taken; how the insider gained access to the target; and how he or she was persuaded to commit the crime.
- The effectiveness of the security procedures of the corporation, institution, or agency, specifically those implemented to prevent insider crime; and the changes in those procedures that may have resulted from these crimes.

## METHODOLOGY

While insiders could play a critical role in the planning or execution of a crime against a nuclear facility, they have not done so thus far, according to the public record. Because there are no empirical data on nuclear incidents, this study relies primarily on data derived from analogs to insider nuclear crimes—i.e., crimes with characteristics that would be likely to appear in nuclear crimes, such as vandalism, major theft, and crimes motivated by emotional instability or ideology.

We are under no illusions that this examination of reported insider crimes will reveal a pattern of potential nuclear insider crimes. To begin with, in none of our cases was attention to security comparable to that exercised at a DOE facility. Also, some of the incidents—those that occurred at fairly well-guarded targets, those that required elaborate planning, or those motivated by ideology—are more analogous to

[1]John P. Clark et al., *Theft by Employees in Work Organizations*, Minneapolis, MN: Department of Sociology, University of Minnesota, June 30, 1981.

[2]Insider crimes are crimes that an employee commits against his or her employer. The term "hostile employee" is used synonymously with "insider" throughout this study.

potential nuclear crimes than are others. But we have chosen to include insider crimes having even a single attribute that might apply to a potential nuclear crime because we are attempting to understand the problem of insider crime in general. We hope to discover, for instance, what motivates insiders, what sorts of crimes they commit, and how they interact with other criminals, to enable us to assess their threat to the nuclear domain.

A previous RAND report concluded, "The hostile employee is generally trusted, has knowledge of vulnerabilities, has access to both information and facilities, can often operate undetected for long periods of time, and, having turned against the system or employer, may carry out malevolent actions with the self-righteousness and zeal of other kinds of fanatics."[3] Accordingly, a better understanding of the insiders and the nonnuclear crimes they have helped to perpetrate may enable us to prevent similar incidents in the nuclear arena.

We developed the database used in this study in two stages. In the first stage, we located the relevant cases in two existing RAND databases; one included a chronological listing of 292 anti-nuclear actions in the United States, and the other, compiled in 1980, included 121 sophisticated and high-value burglaries, robberies, and other "conventional" crimes that we considered possible analogs to nuclear crimes.

In the second stage, we compiled a new database that included the relevant pre-1980 cases and material on task force crimes,[4] as well as new information on crimes involving insiders that occurred subsequent to 1980. We collected the recent data from open sources, including press clippings, journal articles, on-line data sources, and published reports. We also interviewed police detectives who conducted the investigations of some of the insider crimes. Initially, 97 incidents were selected for the database. However, 22 of these incidents were rejected, primarily (though not exclusively) because not enough information was available in the public record to pursue the case or because the case was unsolved and therefore the role of the insider and his or her motivations were unclear.

We conducted telephone interviews with head security personnel and managers at the companies, institutions, and government agencies that had experienced the crimes in the database. All were advised that their anonymity would be preserved and that all identifying data in the research files would be destroyed once research was complete. (This is the usual RAND research practice.) Each contacted party was asked

[3]Gail Bass et al., *Motivations and Possible Actions of Potential Criminal Adversaries of U.S. Nuclear Programs*, The RAND Corporation, R-2254-SL, February 1980, p. 28.

[4]Task force crimes are those whose complexity demands the cooperation of a team of operatives.

the following questions:

1. How long had the insider been with the company?
2. What was the apparent motive behind the incident?
3. What screening procedures or background checks were in place when this employee was hired?
4. What in-house or externally contracted security measures were being employed at the time of the incident?
5. Did the insider act alone, or with accomplices?
6. Who initiated the incident (e.g., was the employee approached by outsiders, or did the insider approach the outsider)?
7. If the insider did not initiate the incident, what convinced him or her to take part (e.g., cooption, coercion, blackmail, free will, etc.)? If he or she initiated the incident and did not act alone, how did he or she enlist assistance (either inside or outside the company)?

As a result of these telephone interviews, 13 incidents were eliminated from further consideration because we were unable to elicit corporate or institutional cooperation. The majority of the negative responses came from armored-car companies and banking institutions, which seemed to fear possible negative financial or publicity repercussions. Many of the other negative respondents had suffered from bad press coverage at the time of the incident in which they were involved and wished to avoid any further attention being drawn to their security failures.

The remaining 62 incidents were then divided into three categories for analysis:

- Crimes committed by insiders conspiring with outsiders.
- Crimes committed by insiders conspiring with other insiders.
- Crimes committed by lone insiders.

We believe that terrorists or foreign agents—or even professional criminals—who have access to the help of an insider would be more likely to attempt a crime against a nuclear facility than would a group of insiders or an insider working alone. We have nevertheless included the single insider in our study to examine the characteristics of insiders, and the insider conspiracy group to learn more about both insiders and the nature of conspiracies. Because our sample of cases is selective, the results should be viewed as descriptive. The sample does not represent all conspiracies, and it is not possible to make predictions about potentially dangerous insiders based on these results. With the limited data available, we can only describe the crimes that appear

analogous to possible insider nuclear crimes and report any characteristics they share.

## THE LITERATURE ON INSIDER CRIMES

Throughout this report we refer to and compare our results with three earlier works: Bass et al. (1980), Reinstedt and Westbury (1980), and Mullen et al. (1980).[5]

Bass et al. describe a broad study of the threat that all types of criminal adversaries (ideologically motivated outsiders, economically motivated outsiders, arsonist outsiders, hostile employees, etc.) pose to U.S. nuclear programs. A small section of the study focuses on the threat posed by hostile employees, who are categorized as either (1) emotionally unstable, (2) disillusioned, (3) frustrated, (4) self-serving, (5) in labor-related situations, (6) agents, (7) acting for idiosyncratic reasons, or (8) coerced.[6] Short character summaries are given for each of the eight categories, and predictions are made about the types of hostile actions in which they might engage.

Reinstedt and Westbury analyzed a database of 121 sophisticated and high-value burglaries, robberies, and other "conventional" crimes that were regarded as analogous to potential nuclear crimes. The database included 36 crimes committed by insiders, for which information is given on the number of perpetrators, the value of any stolen items, the type of crime, whether violence was used, and whether employees were coerced or blackmailed into participating.[7]

The Mullen et al. study sought to (1) determine the characteristics of potential insider adversaries to licensed nuclear activities, (2) examine security system vulnerabilities to insider adversaries, and (3) assess the effectiveness of techniques used to detect or prevent insider malevolence.[8] The findings were based in part on 115 insider crime cases, 45 of which had taken place in "strong" safeguard environments and were therefore considered highly analogous to potential crimes against nuclear programs, and in part on opinions expressed by

[5]Bass et al., *Motivations and Possible Actions of Potential Criminal Adversaries*, op. cit.; Robert Reinstedt and Judith Westbury, *Major Crimes as Analogs to Potential Threats to Nuclear Facilities and Programs*, The RAND Corporation, N-1498-SL, April 1980; and S. A. Mullen et al., *Potential Threat to Licensed Nuclear Activities from Insiders (Insider Study)*, Division of Safeguards, Office of Nuclear Material Safety and Safeguards, U.S. Nuclear Regulatory Commission, NUREG-0703, Washington, D.C., July 1980.

[6]Bass et al., p. 29.

[7]Reinstedt and Westbury, p. vi.

[8]Mullen et al., p. iii.

industry and government experts. Mullen et al. created character sketches of four categories of hostile employees ("typical insider thieves, typical insider saboteurs, insiders in a strong safeguards environment, and insiders in a weak safeguards environment").[9]

We also reviewed a substantial body of criminological literature concerning white-collar (i.e., insider) crime. Social psychologists and criminologists (e.g., Sutherland (1949), Cressey (1953), Geis and Meier (1977), Stotland (1977), and Nettler (1982)) have addressed the motives behind hostile employee behavior and the general characteristics of organizations that appear to be prone to such employee activity.[10] However, these studies were of little assistance in our research. In general, they focus on small-scale insider crimes (e.g., employees stealing business supplies, low-value thefts from retail stores, etc.) or corporate crimes that are not analogous to theft or sabotage of nuclear facilities.

## STRUCTURE OF THE REPORT

Section II examines the characteristics and motivations of hostile employees and discusses the effectiveness of various security procedures in preventing insider crime and identifying potentially hostile employees. Section III presents a composite profile of insider criminals. It also identifies trends common to each of the three insider crime categories defined earlier and highlights differences among them. Section IV considers ways in which a terrorist organization or a group working with a foreign government might attempt to obtain the assistance of an insider. The report contains two appendixes: Appendix A briefly describes the 62 incidents that constitute our database, and Appendix B summarizes changes in security procedures that have been adopted by businesses, corporations, museums, military installations, and governmental agencies following criminal incidents.

---

[9]Ibid., pp. 1-3, 1-5.

[10]Edwin H. Sutherland, *White Collar Crime*, New York: Dryden Press, 1949; Donald R. Cressey, *Other People's Money*, Glencoe, IL: Free Press, 1953; Gilbert Geis and Robert Meier, *White-Collar Crime: Offenses in Business, Politics and the Professions* (rev. ed.), New York: Free Press, 1977; Ezra Stotland, "White Collar Criminals," *Journal of Social Issues*, Vol. 33, 1977; and Gwynn Nettler, *Explaining Criminals*, Cincinnati, OH: Anderson, 1982.

# II. THE THREE CATEGORIES OF INSIDER CRIME

The characteristics of the "typical insider" are difficult to pinpoint. For example, some individuals who are not very good at their jobs tend to be tempted to commit crimes against their employers, while other insiders are model employees who are never late and rarely take vacations. This section explores the characteristics and motivations of insider criminals who work in league with outsiders, insiders who conspire among themselves, and lone insiders. Within each of these categories, we also discuss the effectiveness of various security procedures in preventing crime and identifying potentially hostile employees.

## INSIDER/OUTSIDER CRIMES

Insiders conspired with outsiders to commit 32 of the 62 crimes in our database. The outsiders ranged from crime ring kingpins to members of ideological extremist groups, but most of them were simply friends or relations of the insiders. Together, the insiders and outsiders robbed banks; stole checks, microchips, and aircraft parts; manipulated computer accounts; smuggled drugs; misused privileged information; and rigged a lottery, among other misdeeds. They did not, however, commit a single act of vandalism. Those who might have been motivated to wantonly destroy property because of anger toward their employers or dissatisfaction with their situations sought revenge through financial gain at their employers' expense; and those who might have justified vandalism with ideological reasons chose targets that could supply them with funds or information rather than help them to publicize their political views.

### Identifying the Insider

We were able to ascertain the ages of 30 of the 49 insiders in our database who worked with outsiders, and we found that nearly half were under 30 years of age[1] (see Table 1). Of these, 14 were between

[1]This is consistent with the findings of a 1986 study of insider crimes against the Service Merchandise Company reported in Michael H. Miller, "Portrait of a Thief as a Young Man," *Security Management,* Vol. 30, No. 6, June 1986, pp. 38–42.

the ages of 19 and 29, and the rest were spread almost evenly between 30 and 59 years of age: six were between 30 and 39, five were between 40 and 49, and five were between 50 and 59.

It is difficult to determine whether youth itself encourages insider crime or whether the involvement in crime reflects a lack of commitment to jobs and employers. One security director suggested that young employees may lack commitment because they are less likely to have family responsibilities and are more mobile than middle-aged employees. As a result, they may tend to be less dependent on a stable job.

Young employees may also be less loyal to their employers simply because they have not worked for them very long. According to Lipman and McGraw (1988), "Employees who felt a long-term commitment to the employer were less likely to steal than those without such a commitment."[2] Slightly more than half of the insiders under 30

**Table 1**

**CHARACTERISTICS OF INSIDERS WHO CONSPIRE WITH OUTSIDERS**

| Characteristic | Number of Insiders | Percent of Insiders |
|---|---|---|
| Age (N = 30) | | |
| 19 to 29 | 14 | 47 |
| 30 to 39 | 6 | 20 |
| 40 to 49 | 5 | 17 |
| 50 to 59 | 5 | 17 |
| Length of Employment (N = 24) | | |
| Less than 1 year | 8 | 33 |
| One to 3 years | 3 | 13 |
| Four to 10 years | 9 | 37 |
| Over 10 years | 4 | 17 |
| Job Type (N = 48) | | |
| Managers/supervisors | 7 | 14 |
| Operations | 31 | 65 |
| Guards | 10 | 21 |
| Motives (N = 34) | | |
| Self-serving | 32 | 94 |
| Ideological/self-serving | 2 | 6 |

[2]Mark Lipman and W. R. McGraw, "Employee Theft: A $40 Billion Industry," *Annals*, AAPSS, No. 498, July 1988, pp. 51–59.

years of age about whom we had information on length of employment were employed for only a short period. Four young insiders had worked for three years or less, and two of these had been employed only a few weeks. However, one 27-year-old had been employed for five years, a 29-year-old had worked for seven years, and a 28-year-old had worked for eight years at the bank from which she stole.

The correspondence between extremely short-term employment and insider crime is striking: 8 of the 24 insiders for whom information on length of employment was available had been employed less than a year, while two others had been employed less than two years. The Nuclear Regulatory Commission (NRC) found in 1980 that crimes committed by offenders in conspiracies[3] rarely occurred within the insider's first two years of employment.[4] One insider in our database was employed for three years, bringing the total of short-term employees (those who worked three years or less) to 11. Nine insiders were employed from five to eight years, a result roughly consistent with the NRC finding that more than half of the insiders who acted in conspiracies had worked for their employer for six to ten years.[5]

Even a long-term commitment does not guarantee that employees will not succumb to the temptation to steal. Four insiders had worked for over 10 years for the companies they swindled or robbed. One of these had been employed for 17 years, and one for 19 years. A security director stated that he is wary not only of new, young employees, but also of those who have worked many years for the company. Long-term employees, he explained, may be angry, believing they have been overlooked for promotions, or fearful that the company has not adequately provided for their retirement.

Years of employment are not the only indicator of a worker's commitment to a company. The degree to which the employee's success is bound up with the company's success, roughly determined by the employee's level of responsibility within the company, also determines commitment and loyalty.

We have divided the insiders into three groups: those whose function within the company was operational, those who were strictly guards, and those who were managers. One insider was not included in any of these groups because he had been fired for tardiness a few weeks before he committed his crime and therefore did not hold any of the

[3]The NRC study defines a conspiracy as a "secret agreement," understanding, or cooperation between two or more individuals for an illegal or deceitful purpose; a conspiracy may involve individuals both inside and outside a plant or facility. (See Mullen et al., p. D-1.)

[4]Ibid., p. 3-6.

[5]Ibid.

three positions at the time of the crime. (He is included, however, in the assessments of other characteristics of insiders because he acted with information to which he had been privy when he worked for the company as a guard.) Of the remaining 48 insiders, 31 were operational employees (a finding again consistent with the NRC study),[6] 10 were guards, and 7 were managers.

Insiders' positions within the company may determine their access to the goods they steal. Large quantities of money, goods, and, in one case, information passed directly through the hands or before the eyes of operational employees in the companies that suffered insider crimes. One messenger simply carried off the bank certificates he had been sent to retrieve. Managers are often entrusted with codes and keys; a supervisor who burgled her bank in Nevada was able to do so in part because she was familiar with the vault combination. Guards not only have access to the money or goods they are protecting and all areas of the building in which those valuables are stored, they also usually control alarms. Reinstedt and Westbury found that guards participated as insiders in 36 percent of a sample of crimes involving guarded targets.[7] Our data indicate that in companies that employed guards and suffered insider crimes, guards were somewhat more likely than others to be the insiders. Of the 20 crimes in our database involving guarded targets (e.g., banks, armored-car companies, and museums), 9 were carried out with the assistance of guards.[8]

Males were involved in 23 of the 32 insider/outsider conspiracy cases. We cannot evaluate the importance of this male predominance, since we do not know the ratio of male to female employees in every company. However, the pool of possible outside accomplices would presumably contain as many women as men. Yet none of the male insiders worked with female outsiders, and all of the female insiders worked with male outsiders. In one case, male and female insiders, a husband and wife, worked together with male outsiders; the woman introduced her husband to the leader of a crime ring for which he soon began to steal aircraft parts.

To the eight different types of hostile employees described by Bass et al., we added a ninth type, those motivated by ideology. Nevertheless, we were limited in our attempts to fit the insiders in our database into these categories, because we had to discern their motives from newspaper accounts and security directors' opinions. When an employee has stolen millions, we cannot always be certain, for instance,

[6]Ibid.

[7]Reinstedt and Westbury, p. 17.

[8]This figure does not include the ex-guard mentioned above.

that financial gain was the only motive; some of these insiders may have been motivated by emotional instability or by a grudge secretly harbored against the employer. But according to our best reckoning, in nearly every case, the insider's primary motivation was to serve her or himself. There were two exceptions in which financial as well as ideological motivations played a role in the crime (one incident involved a white supremacist terrorist group, the Order, and the other involved a Puerto Rican separatist terrorist organization, *Los Macheteros*).

We divided these self-serving cases into four groups, according to motivation: financial gain, financial gain coupled with ideology, financial need (where we could discern evidence of indebtedness), and personal attachments or intimate relationships. Twenty-two of the crimes were prompted primarily by financial gain. This finding supports Lipman and McGraw's contention that economic necessity is rarely a reason for employee theft.[9] While three insiders in the category did need the money they took (one to cover massive gambling debts and two to buy drugs), lack of money is not the real problem of those who steal to support their habits.[10]

A personal attachment or intimate relationship motivated four, and possibly five, insiders, most of them female. A central vault manager returned to the bank at night to empty the vault, then flew to Paraguay with her boyfriend, who had helped her carry out the theft. A woman who collected Social Security payments for fabricated beneficiaries used her profits to fund her imprisoned husband's appeal. Jealousy partially motivated one insider, who helped a white supremacist group to steal money from the armored-car company where he worked. His former wife, also employed by the armored-car company, was having an affair with a third employee, who was black. The insider not only assisted the white supremacists, he also helped plan the robbery of the truck in which his former wife was working. A woman who embezzled money from a state treasury did so to further the career of a bandleader with whom, authorities speculate, she may have been intimately involved. Finally, a woman who worked for a state tax board, who was also the girlfriend of a member of the Aryan Brotherhood, a white supremacist prison gang, obtained the home addresses of prison guards who were targeted for assassination.

Many of the insiders had several motivations, so their categories overlap. Three of those who were motivated by romantic involvement were also influenced by ideological groups—racist extremist organizations and a religious group. One other insider, whose mother was a

[9]Lipman and McGraw, p. 56.

[10]Ibid.

long-time activist in the Puerto Rican separatist movement, through which she had connections with the Puerto Rican terrorist group *Los Macheteros,* also had some ideological motivation. In this case and the case involving the white supremacist group, while ideology (and in the latter, jealousy as well) encouraged the crime, the insiders' financial acquisitiveness was also well-satisfied. Each was promised a sum of money for his personal use upon completion of the crime. In the two other cases involving ideological groups, the female insiders perpetrated their crimes not to help the groups, but to help men who were members of the groups.

Two of the insiders were frustrated employees. Both were unhappy because they had not received promotions, but neither was motivated solely by disaffection. A bank loan officer who embezzled money to cover bad checks had a complicated motive involving loyalty to a friend and co-worker, misplaced trust, and fear of detection, as well as frustration and financial gain. The other frustrated employee, a U.S. Navy employee who stole aircraft parts, certainly found the promise of financial gain even more enticing than the prospect of revenge against his employer. Both of these crimes extended over several years. The Navy employee could also be considered a foreign agent, since the parts he stole were sold to Iran and he was well aware of their destination.

Prompted by a security director's claim that many insider crimes are now drug-related and by the NRC study's assertion that "drug use or abuse was one of the most frequent motivations for the insider,"[11] we identified six cases involving a total of 16 insiders that had some connection with drugs. In three cases, the insiders needed money to buy drugs. Two cases directly involved narcotics smuggling, and in the other, insiders laundered money for a drug smuggler. In the last case, one of the outsiders was a drug addict. It is possible that drugs were connected with other cases that we attributed to purely financial motivation, since in many cases no information was available on how the criminals planned to spend the money they acquired.

## Characteristics of the Crime

The insider approached outsiders with the idea for the crime in 12 of the 32 cases; outsiders instigated the plan in 9 cases; in 11 cases, the initiator was unclear. Of the 9 cases instigated by outsiders, 4 were suggested by extremist groups: a fraud committed for the leader of the fundamentalist religious sect, a robbery committed for the Order, a robbery committed for *Los Macheteros,* and the collection of addresses

[11]Mullen et al., p. 3-1.

for the Aryan Brotherhood. All of these groups had members who had influence with an insider.

In most cases, there is a tendency to solicit help from people with whom the insider has an established relationship. Nineteen of the insider/outsider crimes in our database were carried out by people who knew each other before the crime was planned. One case involved an employee, her brother, her brother's girlfriend, and the girlfriend's husband. In 10 cases, the participants became acquainted solely to facilitate the crime. We are unsure of the connections between the insiders and the outsiders in the remaining 3 cases. In 24 cases, a single insider worked with outsiders to commit the crime. In the 8 remaining cases, insiders conspired with other insiders as well as with outsiders.

Theft of money was the object in 24 cases; the offenders netted cash, checks, or securities. In one airline crime, both cash and jewels were stolen. In three other cases, goods alone were stolen, including jewels, furs, microchips, aircraft parts, dresses, and museum artifacts. Two cases involved drug-smuggling conspiracies. There was one case of money laundering and one case in which an employee divulged privileged information. These last are two of ten incidents in which the stolen goods were intangible, i.e., no object had to be hidden and carried from the premises. The characteristics of the insider/outsider crimes we examined are listed in Table 2.

Insiders most often exploited security weaknesses that were evident in their daily routines. In 24 cases, insiders had daily access to what

**Table 2**

**CHARACTERISTICS OF INSIDER/OUTSIDER CRIMES**

(N = 32)

| Characteristic | Number of Cases | Percent of Cases |
|---|---|---|
| Crime Type | | |
| Theft/robbery | 22 | 69 |
| Embezzlement | 6 | 19 |
| Drug smuggling | 2 | 6 |
| Other | 2 | 6 |
| Goods Stolen | | |
| Money/securities | 24 | 75 |
| Commodities | 4 | 13 |
| Drugs | 2 | 6 |
| Information | 1 | 3 |
| Services | 1 | 3 |

they eventually stole. A department store housekeeper, for example, had no difficulty finding dresses to steal in the area in which she worked.

In 8 cases, the insider had to contrive a means by which to reach the loot, and a remarkable range of ingenious tricks were devised. Notably, in 6 of these nonroutine cases, the target was tightly secured with locks, alarms, and guards. One company used a thorough screening process, including a check of its applicants' criminal records, along with its other security measures; however, none of the organizations in our database employed security equivalent to that at a nuclear facility. Those companies that were heavily secured were robbed or burgled by insiders using routine access in 13 cases—as many crimes as were carried out by insiders using routine access to steal from companies in which security was lax.

In 9 cases, the insiders in this category supplied their accomplices on the outside with information, causing delays or creating diversions rather than actually stealing the money, goods, or information. Insiders worked indirectly in 3 of 8 cases in which perpetrators use nonroutine access and in 6 of 24 operations that depended upon routine access.

Operational employees participated in half of the crimes that involved nonroutine access. The other half of the incidents were perpetrated by equal numbers of managers and guards. Operational employees participated in slightly less than half of the crimes conducted via routine access, and the remainder was again divided equally between managers and guards. The fact that operational employees formed the majority in each group supports the NRC study's findings regarding insiders acting in conspiracy.[12]

Ten of the crimes that involved routine access were perpetrated in front of other employees without arousing their suspicion, and several of these activities spanned years. With the exceptions of the housekeeper who stole dresses and the lottery tamperers, all of the insiders who used their routine access to the target but were unable to carry out the crime in view of co-workers were guards or drivers. It is not surprising that only one crime requiring nonroutine access could have been perpetrated in front of others without revealing the perpetrators' intent. This single exception was the case of an insider who managed to charm his way regularly into unauthorized areas; thus, although his access to these areas was not included in his normal job, he contrived to make the nonroutine routine.

---

[12]Mullen et al., p. 3-6.

Overall, insiders and outsiders in conspiracy tend to deceive rather than force; however, in 10 cases perpetrators threatened with guns, and in 3 of these the insider himself wielded the weapon. While not all of the companies that were protected by strong security attracted violent crimes, all of the crimes that did involve violence were directed against highly secure targets: banks, armored-car companies, and the cargo holding area of an international airline. Only one of these incidents, the holdup of an armored car by members of the Order, appeared to have required sophisticated planning.

We judged the level of planning in each case on the basis of newspaper, security directors', and police accounts of how difficult it was to circumvent or overcome the organization's security, how many variables the offenders had to control, and how much time the conspirators needed before the plan was ready to implement. The majority (19 incidents) appeared to demand very little preparation, but 12 others seemed to be carefully plotted. We lacked information with which to estimate the planning level in one of the cases. Of the 8 crimes that extended over months or years, 3 were highly planned and 5 were not. In most cases, the success of the crime seemed to depend not so much upon expert planning and execution as upon security flaws.

## Security Procedures and Deficiencies

Although none of the corporations, institutions, or government agencies in our database exercised the security that would be necessary at a nuclear facility, those 23 that employed guards and used alarms to protect their valuables were considered to have high security levels. A total of 9 companies either maintained little security, merely subjecting applicants to an employment screening and checking their work with audits, or paid no attention to security.

"The company always employs a number of potential thieves and my job is to make them afraid to act upon their impulses," asserts one security director. His company has long maintained a high level of security specifically intended to foil insiders, but few other organizations in our database were particularly conscious of an insider threat until they suffered an insider crime. In the case of the lottery tampering, for example, the organization had absolutely no protection from insiders. Six companies had security procedures that existed only in theory, and this actually contributed to the success of the crimes. A security director in an international airline stated in the NRC report: "Most high value losses are not system failures, but the failure of peo-

ple to adhere to the system."[13] An insider was able to divert funds from the Social Security system into her own purse for years because prescribed audits were never performed. In one of the armored-car company crimes, codes that opened the vault and were supposed to be kept secret were instead freely broadcast and written inside employees' lockers. An insider was allowed access to unauthorized areas in a naval aviation depot. A Nevada bank supervisor was able to burgle the vault at night because the bank failed to enforce its policy requiring that the vault could not be opened by a single employee. In another bank case, a teller pretended that two of his friends were holding him hostage; the security director insisted that the crime would not have been successful had security procedures been followed, but he would not specify the nature of those procedures. An electronics company from which a guard and an outside crime ring stole microchips neglected to subject that guard to its usual employment screening. (Background checks are discussed in more detail below.)

Even if security procedures had been rigorously followed, they might have proven inadequate in at least 4 cases and certainly were so in 12 other cases. These 16 organizations all might have deterred the crimes they experienced if they had used additional security measures.[14] The 16 organizations were lax in six specific areas:

- Three employers would have benefited from careful accounting. Inventory checks might have caught the insider at the naval aviation depot, and auditing would have exposed the crimes of the embezzler who cleared bad checks and the one who skimmed money from the state treasury.
- Three organizations were victimized because of misplaced trust in impostors; they failed to verify the insiders' identities and appropriate whereabouts. One bank supervisor gave her accomplices uniforms so that they could pass as guards. In one armored-car company case, a man who had been fired from his position as a guard persuaded legitimate guards to let him enter a building. In another, a man who worked at one branch of an armored-car depot convinced employees at another branch that he was supposed to work with them for the day. This insider also had planted an outsider whom he had disguised as an employee in the building.

---

[13]Mullen et al., p. 4-2.

[14]This is not to suggest that the remaining 16 cases were as secure as possible; we simply do not have enough information to determine what flaws existed in the security procedures.

- A lack of offsite alarms facilitated the crime in five cases. Three involved guards who were left alone with valuables and allowed outsiders in to steal them. One was the case of the bank supervisor who opened the vault at night, and one was the theft of valuables from an airline's holding area.
- Five crimes might have been discouraged if more than one person had been responsible for the safety of the target. In two of these cases, a guard had been assigned to work alone. One case was the electronics company theft, and the other involved the guard of an armored-car company warehouse who claimed to have been surprised by gunmen while he was watching television. The third case was that of the bank supervisor who should not have been able to open the vault alone. The fourth case was that of the naval aviation depot, where the insider had complete control over the movements of the parts he took. Finally, the woman who embezzled money from a state treasury managed to continue in her crime for years because she refused to let anyone learn the procedures involved in her job.
- Inadequate supervision assisted the perpetrators in six cases: the lottery, the department store from which dresses were stolen, the postal center from which checks were taken, the naval aviation depot, the airline with the smuggling passenger agent, and the armored-car company that allowed impostors to work for two hours.
- Relaxed restrictions on access to critical areas made three crimes possible: the naval aviation depot theft, the case in which two brothers hid in the cargo area of a plane, and the case in which skycaps smuggled drugs through Customs.

Many security directors claim that thorough background checks are more useful than internal procedural controls in preventing insider crimes. (Similarly, periodic background checks of employees might also prove helpful in deterring insider crime by identifying employees with potential financial or psychological problems.) Eleven companies that were robbed or burgled by insiders working with outsiders had a policy of screening applicants before hiring them, but in six cases this screening involved only a check of the applicant's former employers, and in one case, the screening policy was not carried out. The security director of the electronics firm from which the computer microchips were stolen admitted that although company policy stipulated that all potential employees be subjected to a reference check, the screening probably was not performed. This would seem to be a significant lapse, since the guard who facilitated the crime had been fired from his

previous job for dealing in drugs; however, since federal and state restrictions prohibit previous employers from divulging reasons for dismissal, a legal screening actually would have made little difference in this case. It also underscores the point made by an airline security official in the NRC report that most high-value losses are not system failures, but people failures.

Three organizations had conducted a thorough screening of the insiders who committed the crimes, including a check for criminal records.[15] In one case, because of federal and state restrictions, this check was performed through informal contacts with the local police. This company also subjected its applicants to a polygraph test and required them, over a period of time, to complete several questionnaires asking for the same information. Inconsistent answers to these questionnaires, the company reasoned, were likely to indicate lies. These thorough background checks were not especially successful, however. While one of the four insiders who had been subjected to a background check was employed for 17 years and so may have changed considerably since the time when he was screened, two had worked only 3 years each when they participated in crimes. We were unable to ascertain the length of employment of the fourth insider.

Complaining that legal restrictions on access to criminal and employment records kept them from securing their businesses against insider crime, four companies bolstered their screening processes to include informal contacts with the security directors of other businesses for access to reasons for termination and with police for access to criminal records. One organization's new screening system includes such extensive procedures as maintaining a team of employees to do nothing but run detailed background checks. This team asks applicants to complete two applications so that the security department may compare them for discrepancies; it administers a psychological examination that is supposed to expose drug and alcohol habits, dishonesty, and tendencies toward absenteeism; and it checks civil, driving, and criminal records through a network of informal contacts. The inclusion of police contacts seems to be of only marginal utility, since in only one case, that of the microchips theft, would this sort of screening have been likely to help the company avoid the crime. This finding is particularly relevant to the Department of Energy, which can make a thorough check of its applicants' police records. Clearly, however, such checks do not guarantee that potential insiders will be identified. Although, as Bass et al. state, "professional criminals are

[15]The U.S. Post Office may examine criminal records at its discretion, but it is unlikely that it did so in the cases in our database.

unlikely to secure the more sensitive jobs in nuclear facilities,"[16] very few insiders are professional criminals.

If, as security directors claim, a thorough background check can weed out applicants with histories of drug or alcohol abuse and psychological instability, such a check might have eliminated the state treasury embezzler who developed hysterical amnesia and the bank teller who stole from her employer to support her drug habit. On the other hand, the museum guard who stole to buy drugs had been subjected to a thorough background check. Several security directors maintained that watching for changes in attitude, performance, dress, and even haircut is essential for identifying potential thieves, because such signs can indicate a change in lifestyle and the resulting need for more money. Continuing supervision, along with periodic screenings, including credit checks, might have alerted security personnel to two airline employees, one of whom needed money to cover massive gambling debts; the other used some of his smuggling profits to throw elaborate parties at which cocaine and other drugs were regularly used.

Even if the background check could predict an applicant's tendency to be chronically dishonest, late for work, addicted to drugs or alcohol, or subject to blackmail or financial problems, it could not identify those who will succumb to temptation rather than be honest when the chance arises. As Bass et al. point out, "the amateur criminal or opportunist—the employee who will seize the chance to cash in on a fortuitous opportunity—probably can't be identified in advance."[17] Even if he has committed the same crime before, background checks probably will not reveal the fact, in view of legal (e.g., libel) considerations which limit frank assessments or the communication of relevant—though derogatory—information concerning a prospective employee or the reduction of serious charges to lesser offenses through plea-bargaining. Background checks are also unlikely to uncover characteristics that might lead an employee to join a hostile ideological group or to commit a crime for reasons of principle or personal relationships.

## INSIDER CONSPIRACIES

Insiders engaged in conspiracy constitute the smallest category in our database. Insider conspiracies committed only 12 crimes, including theft, armed robbery, vandalism, and embezzlement.

---

[16]Bass et al., p. vii.

[17]Ibid.

## Identifying the Insider

The insider conspiracy crimes involved as few as 2 and as many as 50 employees, often of vastly different ages. In many instances, information on the age of individual perpetrators was, in fact, unavailable. Therefore, the average age of perpetrators in this category is of no descriptive value. However, some insight into the most common age of the conspiratorial insider can be gained by dividing the insiders involved in each incident into age groups spanning 10-year increments. For example, in one incident there were four perpetrators—two between 20 and 29 years of age, one between 40 and 49, and one between 50 and 59. Thus we made one entry in the 20–29 category (despite the fact that two persons were involved), one in the 40–49 category, and one in the 50–59 category. We find that persons between 20 and 29 years of age committed six of these incidents, as shown in Table 3; persons between ages 30 and 39 were responsible for only two incidents; persons aged between 40 and 49 were responsible for three incidents; and persons between the ages of 50 and 59 years were responsible for four incidents.

The length of time that the insider was employed before the commission of a work-related crime was clearly weighted toward either an especially short period of employment (3 years or less) or a long period (more than 10 years). Information on length of employment was available for only 9 of the 12 incidents in this category, and in each case we determined an average length of employment for the insiders involved. No incidents occurred among persons who had been employed between 4 and 9 years; in contrast, the NRC study found that more than half the crimes committed by insiders in conspiracies occur between the sixth and tenth year of their employment. In five of our cases, insiders were employed for 3 years or less (three for 1 year or less, one for 18 months, and one for 3 years) at the time of their crime; in four cases, insiders were employed for more than 10 years (in one case for 17 or 18 years, and in the other three for 10 to 14 years). This distribution is similar to that of the insider/outsider category, in which most of the crimes were committed by persons under the age of 29 (who, one may presume, had been employed for short periods of time), followed by persons over age 50 (who are likely to have worked for the same employer for long periods of time). In only two incidents in this category were women involved (the woman who conspired with her husband to embezzle funds from the post office and the head supervisor who conspired with window clerks at a post office to steal money).

More than half of the incidents were committed by operational employees engaged in normal daily operations; managerial/supervisory

Table 3

CHARACTERISTICS OF INSIDERS WHO CONSPIRE WITH OTHER INSIDERS

| Characteristic | Number of Insiders | Percent of Insiders |
|---|---|---|
| Age (N = 15)[a] | | |
| 20 to 29 | 6 | 40 |
| 30 to 39 | 2 | 13 |
| 40 to 49 | 3 | 20 |
| 50 to 59 | 4 | 27 |
| Length of Employment (N = 9) | | |
| Less than 1 year | 3 | 33 |
| One to 3 years | 2 | 22 |
| Four to 10 years | 0 | — |
| Over 10 years | 4 | 44 |
| Job Type (N = 15)[a] | | |
| Managers/supervisors | 4 | 27 |
| Operations | 9 | 60 |
| Guards | 2 | 13 |
| Motives (N = 12) | | |
| Self-serving | 11 | 92 |
| Altruism/idealism | 1 | 8 |

[a]The number of insiders is greater than the number of crimes, and each crime could involve any combination of categories listed. Percentages are based on the number of crimes and may total to more than 100.

personnel participated in four incidents, while guards participated in only two. The low number of insider crimes in this category involving guards supports Reinstedt and Westbury's conclusion that guarded targets are not particularly susceptible to insider crimes.

The overwhelming motivation of the insider criminals in this category was financial gain: self-serving intentions involving money accounted for 11 of the 12 incidents. To accommodate the remaining case in this group, we again added a motivation to the eight defined by Bass et al., altruism and idealism. This motive applied to the vandalization of fuel at a commercial nuclear powerplant to draw attention to what the vandals alleged were unsafe storage practices. Three of the insider crimes were drug-related: Two were perpetrated in order to obtain money with which to purchase drugs, while the other involved narcotics smuggling. This finding corroborates the conclusion reached by the NRC study on the frequency with which drugs are connected

with insider crime and with the similar observations of many corporate security directors.[18]

## The Characteristics of the Crime

Ten of the 12 insider crimes in this category involved the theft of tangible items, ranging from cash and jewelry to military equipment to postage stamps and commercial merchandise. Cash and/or jewelry figured in six of the insider crimes, and merchandise or other commercially marketable items figured in the remaining four. Two of the crimes involved vandalism and smuggling, as shown in Table 4.

Pairs of insiders committed four of the incidents; 5 or fewer persons, between 6 and 10 persons, and 50 or more persons were involved, respectively, in two incidents each; and 11 persons were responsible for one incident.[19]

In no instance in this category was the insider's cooperation coerced or otherwise forcibly obtained (either by threat or actual violence) by his fellow conspirators. The only case involving coercion of any sort was that of the baggage handlers' cocaine smuggling ring. However, the coercion consisted only of intimidating fellow workers who were

**Table 4**

**CHARACTERISTICS OF INSIDER CONSPIRACY CRIMES**
(N = 12)

| Characteristic | Number of Cases | Percent of Cases |
|---|---|---|
| Crime Type | | |
| Theft/robbery | 9 | 75 |
| Embezzlement | 1 | 8 |
| Drug smuggling | 1 | 8 |
| Vandalism | 1 | 8 |
| Goods Stolen[a] | | |
| Money/securities | 6 | 50 |
| Commodities | 4 | 33 |
| Drugs | 1 | 8 |
| No tangible item | 1 | 8 |

[a]Percentages are based on the number of goods stolen and may total more than 100 because of incidents involving thefts of multiple types of goods.

[18]Mullen et al., p. 3-1.

[19]See Table 3.

not part of the conspiracy but had heard or knew of it into keeping quiet. This is a separate issue from that of coercing an insider to become involved in an actual crime. One case confirms the suggestion of Bass et al. that individuals might infiltrate a company specifically intending to assist in a crime.[20] In this case, a father who had recently been promoted to a supervisory guard's post as captain used his position to process the son's employment application under an alias (because of the son's criminal record in another state) and to place him in a position in which the two could carry out the robbery of an armored car.

Not surprisingly, the overwhelming majority of insider conspiracy crimes were committed by co-workers. The relationship between the perpetrators may have been personal as well as professional. However, in only two cases (the sabotage of fuel at a commercial nuclear energy facility and an incident involving two postal clerks) could it be determined that a prior friendship may have been the basis on which the conspiracy was predicated. Only two incidents involved close relatives employed at the same place (the father and son armored-car robbers and the husband and wife managers of a postal contract station).

The vast majority of incidents were "targets of opportunity," that is, situations in which the crime could be easily committed without sophisticated planning. Indeed, the two incidents that did reflect at least some planning—the father and son robbery of the armored car and the vandalizing of the commercial nuclear facility—fall far short of requiring or reflecting "a professional approach and . . . a great deal of planning,"[21] which Reinstedt and Westbury noted as characteristics of "task force" crimes. Most of the crimes reviewed were so easy and uncomplicated that in only one instance (the father and son armored-car robbery) was there any violence. Each of the insiders had routine access either to the item(s) they wished to steal, the item they wished to vandalize, or the container in which the narcotics were smuggled.

The crimes in this category involved only insider conspiracies, but various types of "outsiders" did play some role. In half of the incidents, outsiders were involved as "fences" or recipients of stolen items. While there appears to have been no initial collusion between the insiders and the outsiders, the commission of the crime seems to

[20]Bass et al., p. 18.

[21]Reinstedt and Westbury, p. 2. The NRC insider report observed that "in a strong safeguards environment . . . more reliance is placed on non-routine access to the target in combination with covert activity" (p. 1-4), which did not hold true in the case of the fuel vandalization.

have been dependent on the availability of an outsider who was willing to buy or take receipt of the stolen goods. This was the case in the two incidents involving the theft of military equipment by U.S. Marines and by Army soldiers and National Guardsmen; in the smuggling of narcotics into the United States by airline employees; in the theft of stamps slated for incineration by sanitation men; in the theft of jewelry from parcels by two postal clerks who wanted to purchase drugs; and in the theft of merchandise and travelers checks from U.S. mail bags by airline employees. Equally significant, however, in half the insider conspiracy crimes, the perpetrator stole items or money that was of direct value or use and in such a manner that no "outside" conduit was required.

### Security Procedures and Deficiencies

To assess the security procedures that might have prevented crimes in this category, we shall briefly review the security characteristics of the individual incidents that pertain to insider crimes:

- In both cases involving the theft of military equipment, strict inventory control was not maintained. Personnel were able to check out equipment and not return it because (1) those in charge of inventory were involved in the crime, and (2) inventory control in general was quite slipshod.
- In the theft of coins from parking meters by the guards of a private security firm employed to carry out the collection, there was inadequate supervision, especially since the on-the-spot supervisors were involved in the crime.
- At the U.S. Government Federal Reserve facility, there were no security measures whatsoever, not even the use of supervisory personnel or background checks. The crime was discovered only after a routine audit revealed that employees had stolen more than $60,000 in coins and currency over a 2-year period.
- Procedures for the hiring of the baggage handlers involved in the narcotics smuggling incident varied. Although there was a customary check of employment history, it was not very detailed.
- The only infiltration was abetted by a father in a supervisory capacity at an armored-car company who was able to circumvent the normal background check that would have revealed his son's conviction for crimes in another state.

- Obviously, very few security measures or screening procedures were imposed on the sanitation men convicted of pilfering stamps that were supposed to have been destroyed.
- The vandalization incident at the commercial nuclear energy facility was perpetrated by two ex-"nuclear Navy" men who had been thoroughly screened in accordance with the procedures recommended by the American Nuclear Society. They had also been subjected to the Minnesota Multi-Phasic Test.
- All the U.S. Postal Service employees involved in insider conspiracies had provided the standard three personal and three business references—although the local postmaster may have also done a local criminal records check on his own accord.

Since the insiders had routine access to either the item or the site of the crime in all cases, physical security devices such as off-site alarms were not applicable and would have had no effect. Deficiencies in accounting and auditing contributed to the success of the crime in 2 of the cases. Accounting and auditing, however, led to the discovery of the perpetrators in 4 incidents (the Marine theft of equipment, pilfering at the Federal Reserve bank branch, and 2 post office incidents). Less successful was the exercise of managerial or supervisory functions, where deficiencies directly contributed to the accomplishment of 9 crimes (including 2 thefts of military equipment, the theft of revenue from parking meters, the Federal Reserve theft, the father and son armored-car robbery, the theft of postage stamps by sanitation workers, the vandalization of the nuclear powerplant, and 2 post office incidents).

In the majority of the incidents, insiders were not dependent on a conspiracy in order to gain access to a target; rather, the conspiracy served as psychological reinforcement. Indeed, as Bass et al. noted, "Internal conspiracies may evolve either because of practical necessity (perhaps more than one person is needed to implement a criminal plan) or the need for psychological reinforcement, or both. Youngsters' penchant for saying 'I'll do it if you will' carries over to the adult world; there, too, people may 'egg each other on.'"[22] In this category, there was a need to involve a specific individual in the commission of only 2 of the crimes—the post office incidents.

Rotation of supervisory personnel would probably have prevented many of the crimes in this category. For example, in 11 incidents, security depended largely on the trust of superiors rather than on any stringent security policies (the nuclear energy incident was the excep-

[22]Bass et al., p. 37.

tion). Thus, the NRC finding that failure to rotate those in authority allows thefts to go unnoticed and to recur is particularly relevant.[23]

In only 3 incidents had the existing security procedures been rigorously enforced. Although employees involved in 9 of the incidents had been subjected to some form of background check, only 1 had been subjected to a *thorough* background check. Inadequate screening actually contributed to the success of 2 of the crimes in this category.[24]

Perhaps only 4 of the incidents could have been prevented by periodic rescreening of employees. Half of the incidents for which we were able to obtain information on the insider's length of employment occurred within 3 years of the employee's hiring, and half occurred after 10 years or more. Of those who were employed less than 3 years, 6 committed crimes within their first year of employment.

## LONE INSIDER CRIMES

Eighteen of the crimes we examined were carried out by an insider with no assistance. The most distinguishing characteristic of these single-insider incidents is the high proportion that are motivated by emotional disturbance. Many of the lone insiders seem to have harbored anger against an employer that neither co-workers nor outsiders could share. Like the other types of insider criminals, the lone insiders most often stole money or goods to sell for profit. The exceptions were one case of arson and one case of planting a virus in the employer's computer system.

### Identifying the Insider

We were able to obtain the ages of 11 of the lone insiders, and, as in the previous categories, youth predominates (see Table 5). Seven were under 30; one was 30; two were between 40 and 50; and one was 57. These insiders also tended to be employed for only short periods. However, unlike the insiders who worked with outsiders, most of these short-term employees had been employed for less than 1 year. In fact, of the 13 insiders about whom we could ascertain length of employment, 9 were employed 3 years or less. Although one man had worked for 20 years for the employer that he cheated, he was the only one who had been employed for more than 10 years. Security officials at a museum that was burgled by a single insider consider long-term

[23]Mullen et al., pp. 4-2 and 4-3.

[24]This corresponds with the NRC's finding that only 15 percent of insider incidents could be prevented by better screening. (See Mullen et al., p. 4-5.)

employment to be a factor militating against insider crime. The department encourages its guards to view their jobs as careers and rewards seniority with choice assignments and shifts, as well as with pay increases.

Again, females played a minor role. There was only one female lone insider in our database, a bank employee who skimmed money from the debit payments she wrote.

Of 17 insiders whose position in the company was known to us, 8 did operational work (see Table 5). One case involved a former operational employee. Five insiders were managers, and 2 of these made specific use of that status in order to commit the crime. The chief of security at a museum dismissed his staff so that he could freely take paintings from the building, and a bank manager was able to hide his illegal money transfers because the tellers did not question his authority when he told them that he needed to borrow their computer terminals and identification numbers. Guards were involved in four of the crimes in this category.

**Table 5**

**CHARACTERISTICS OF LONE INSIDERS**

| Characteristic | Number of Insiders | Percent of Insiders |
|---|---|---|
| Age (N = 11) | | |
| 20 to 29 | 7 | 64 |
| 30 to 39 | 1 | 9 |
| 40 to 49 | 2 | 18 |
| 50 to 59 | 1 | 9 |
| Length of Employment (N = 13) | | |
| Less than 1 year | 2 | 15 |
| One to 3 years | 7 | 54 |
| Four to 10 years | 3 | 23 |
| Over 10 years | 1 | 8 |
| Job Type (N = 17) | | |
| Managers/supervisors | 5 | 29 |
| Operations | 8 | 47 |
| Guards | 4 | 23 |
| Motives (N = 18) | | |
| Self-serving | 12 | 66 |
| Frustration | 2 | 11 |
| Emotional disturbance | 2 | 11 |
| Idiosyncratic | 2 | 11 |

As might be expected, all of the guards used their normal access to the target to carry out the crime, stealing the very thing they were supposed to be protecting. Eight other insiders managed to steal, start a fire, and introduce a computer virus without varying their daily routines or going into unauthorized areas. The NRC study found that single insiders used routine access more often than did those who acted in conspiracies.[25] Our results supported this finding when we compared lone insiders with insiders who conspired with other insiders. However, we also found that insiders who conspired with outsiders used routine access more often than did single insiders.

The desire for money, above all else, motivated the lone insiders to steal. Nevertheless, our finding that 12 (68 percent) of the lone insiders stole for financial gain supports the NRC study's conclusion that fewer single insiders than conspiratorial insiders were motivated by a desire for money,[26] since 85 percent of those who conspired with outsiders and 92 percent of those who conspired with other insiders were motivated by financial gain. One of the 12 lone insiders wanted money for a specific purpose: He was a compulsive gambler.

Two of the insiders were angry with their employers. In the case of a salesman, the reasons for the resentment were unfounded. A company audit proved false his charge that he had not been paid commissions owed to him, and at his trial the judge called for a psychiatric study before sentencing him. Two other incidents involved insiders who were emotionally disturbed. More lone insiders were emotionally unstable than insiders in any other category. In two cases, the motives for the crimes were idiosyncratic: The security director of a museum from which the former chief of security stole paintings speculated that the thief planned to pretend to recover them and be considered a hero. The other insider thought he was dying and wanted to give gifts to his friends and to a home for AIDS patients and to buy a house for himself. This man also said that his employer had not given him his due.

## Characteristics of the Crime

In 11 of the cases, the insiders took or damaged all they wanted in a single operation. In 7 cases, insiders made a habit of stealing periodically, milking their employers until they were caught. In one case, the insider was not detected for 7 years; another was not detected for 10 years. The rest of the long-term crimes continued for a month to a year.

[25]Mullen et al., p. 3-6.

[26]Ibid.

Eight of the lone insiders stole cash, although one complicated the operation by exchanging his money for diamonds, which he then intended to sell for more cash. Eight others took commodities, including gold coins, jewelry, stamps, long-distance telephone access codes, artifacts, paintings, and firearms. All of these items were stolen for their monetary value. Thefts of tangible items accounted for two-thirds of the incidents. Embezzling, the sale of the telephone long-distance access codes, the arson, and the computer-virus incident constituted the remaining crimes. Characteristics of lone insider crimes are summarized in Table 6.

Table 6

CHARACTERISTICS OF LONE INSIDER CRIMES

(N = 18)

| Characteristic | Number of Cases | Percent of Cases |
|---|---|---|
| Crime Type | | |
| Theft | 13 | 72 |
| Embezzlement | 3 | 17 |
| Vandalism | 2 | 11 |
| Goods Stolen | | |
| Money/securities | 8 | 44 |
| Commodities | 8 | 44 |
| No tangible item | 2 | 11 |

Insiders acting alone took, on average, more money than did those working in insider conspiracies, but less than those who worked with outsiders.

We judged only two cases to involve a high level of planning. One of these was the theft of gold, which was described in a newspaper account as "so skillful that the police would not say how it had been done." In the second case, a computer programming consultant's initial wiring of money was fairly simple, but the procedures he followed to launder the money and his negotiations to buy diamonds months before he took the cash indicated a great deal of planning. Only in the arson case, an operation requiring little planning, did a lone insider use violence.

## Security Procedures and Deficiencies

Again, security levels and their enforcement varied widely from company to company. We judged the security at 11 companies, including armored-car companies, banks, and museums, to be generally high; at 7 organizations it was low. Security deficiencies seem to have contributed to the success of at least 12 of the 18 crimes in this category. In five cases, poor auditing allowed thefts to occur unnoticed. In only two of the companies were auditing procedures strengthened after the crime. Two insiders were assisted by a physical weakness in the security structures within the building in which they worked. In one case, a gap in fencing allowed a postal worker to grab registered packages, and in the second case, museum renovations caused paintings to be stored in insecure temporary lockers from which they could easily be stolen, rather than in the secure storage areas normally used.

In at least 12 cases, closer observation of the employee's movements and habits might have helped to prevent the crime. In every case in which insiders exploited their routine access to the target, employers afforded the insiders a great deal of trust and did not closely observe their actions. This, of course, gave the insiders ample opportunity to commit their crimes.

Insufficient screening may have contributed to the success of four of the single-insider crimes; and even a careful employment screening may not have prevented one of the crimes. A previous employer of the insider who worked as a computer security director before planting the computer virus stated that his company had experienced problems with the insider and would not have recommended him. A full screening, in another case, could have exposed the criminal record of the guard who took artifacts from a museum. This museum now has an informal arrangement with the police whereby it can gain access to such records. A periodic screening of at least the credit history of two of the lone insiders might possibly have made employers wary. One of the insiders took money from the post office cash drawer to support his compulsive gambling, and one had complained often of his chronic financial difficulties.

# III. PROFILE OF THE INSIDER

This section considers the three categories of insider criminals in juxtaposition, comparing the data for each group to identify characteristics common to all three groups (that thus present a composite of the typical insider) and characteristics that are different among the three. The conclusions we draw from this comparison should help to define the insider who might pose a threat to a nuclear facility.

## AGE AND LENGTH OF EMPLOYMENT

In 51 percent of all of our cases, the insider was under 30 years of age, but the proportion was slightly lower among insiders who worked with outsiders, as shown in Table 7. Greater age in this group corresponds with a greater percentage of insiders who had been employed over 3 years. Fifty-four percent of the insiders who worked with outsiders were employed for more than 3 years, as were 44 percent of the insiders who conspired with other insiders but only 31 percent of those who worked alone. Those who committed crimes in conspiracy

**Table 7**

**CHARACTERISTICS OF INSIDERS: ALL GROUPS**

(In percent)

| Characteristic | Insider/ Outsiders | Insider Conspirators | Lone Insiders | Total |
|---|---|---|---|---|
| Age | | | | |
| 19 to 29 | 47 | 50 | 64 | 51 |
| 30 to 39 | 20 | 17 | 9 | 17 |
| 40 to 49 | 17 | 25 | 18 | 19 |
| 50 to 59 | 17 | 33 | 9 | 19 |
| Years Employed | | | | |
| Less than 1 year | 33 | 33 | 15 | 28 |
| One to 3 years | 13 | 22 | 54 | 26 |
| Four to 10 years | 37 | 0 | 23 | 26 |
| Over 10 years | 17 | 44 | 8 | 20 |

with outsiders probably did not succumb to the first opportunity for crime that they perceived, but needed an outsider either to supply the idea or to provide support for the crime. The figures in Table 7 also imply that outsiders tended to have more influence over insiders who had been employed from 3 to 10 years than over any other group.

## SEX OF PERPETRATOR

Males were involved in all but ten of the incidents we examined. This may reflect the fact that females tend not to steal property of substantial value in insider crimes (we did not include petty thefts in our database); or employers may be less inclined to publicize cases involving female insiders. The crimes in which women were involved in our database, with one exception (the provision of information to facilitate the assassination of prison guards), consisted only of theft/robbery and embezzlement. Considering their low incidence overall, women constituted a fairly high percentage of the embezzlers (36 percent). They were involved in theft or robbery in only 12 percent of the cases. These figures correspond with those published in a U.S. Department of Justice study which reported that 41 percent of the embezzlers convicted of federal crimes in 1985 were women, and 13 percent of the non-white-collar crimes were perpetrated by women.[1]

More females acted as insiders in crimes that involved outsiders than as conspirators with insiders or lone insiders. All but one of the women was intimately involved with her conspirator. The woman who acted in an insider conspiracy was married to her conspirator.

The distribution of crime types, by sex, is summarized in Table 8.

**Table 8**

**DISTRIBUTION OF CRIME TYPES, BY SEX**

| Crime Type | Number of Crimes | Male (percent) | Female (percent) |
|---|---|---|---|
| Theft/robbery | 43 | 88 | 12 |
| Embezzlement | 11 | 64 | 36 |
| Vandalism | 3 | 100 | 0 |
| Smuggling | 3 | 100 | 0 |
| Other | 2 | 100 | 0 |

[1]U.S. Department of Justice, Bureau of Justice Statistics Special Report, *Federal Offenses and Offenders: White Collar Crime*, 1985, p. 7, Table 14.

## EMPLOYEES' RESPONSIBILITIES

Operational employees acted as insiders most often in every group. In part, this is probably a function of the disproportionately large number of operational employees working at the companies that suffered insider crimes, except in the cases of armored-car companies, where guards would predominate. It is also reasonable to expect fewer offenders among managers, because they are, in general, granted greater responsibilities and remuneration than are operational employees and so may have fewer promotion and salary frustrations. Also, one would expect that those in positions of greatest trust were promoted to those positions because they demonstrated loyalty. Guards, of course, were not employed by every company in the database, which explains their small numbers in this sample of all incidents. Of the crimes that did take place at guarded targets, guards committed 41 percent.

Crimes committed by operational employees were most frequent in the insider conspiracy group, which is to be expected, since operational employees are more likely than managers or guards to perform their routine work in teams. Working with each other daily would allow these employees to develop trust in one another, which would not only make proposing the idea for a crime to a co-worker and committing it with him or her less risky, but would also be a source of psychological support. If these suppositions are true, it is not surprising that managers, who do not generally work in groups, committed crimes alone or with outsiders far more often than they did with other employees.

## MOTIVATION

The overwhelming majority of insiders in all groups committed their crimes for financial gain. This is true even in the two incidents that involved terrorist groups and the one that involved a foreign government. The insiders in these cases predicated their assistance not on ideological affinity or sympathy alone, but on the additional incentive of a promised monetary reward, i.e., part of the "take." These examples, as well as the sheer weight of the self-serving motivation in insider crimes overall, suggest that a terrorist group could secure an insider's assistance simply by paying him or her.[2]

[2]Financial gain, not ideological sympathy, has been the primary motivation behind U.S. citizens convicted of acts of espionage against the United States on behalf of various Communist bloc countries—the Walker family and Christopher Boyce (of "Falcon and Snowman" fame), among others. See Permanent Select Committee on Intelligence,

The greatest number of crimes that were not motivated by the desire for financial gain were committed by lone insiders. On the whole, lone insiders appeared to be less stable than people in the other groups; one-third of the lone insiders were motivated by emotional disturbance, frustration with their employment, and idiosyncratic reasons. With their tendency to act inappropriately on the basis of their feelings, it would seem that these individuals could be easily co-opted by terrorists; but unstable people are, according to our results, seldom persuaded to commit crimes with others. It may be that other insiders do not trust them, and outsiders cannot easily identify them.

## DURATION OF CRIMES

Overall, 46 percent of the crimes were committed over an extended period of time, and 54 percent were confined to a single event—fairly equal proportions. However, the three groups display marked differences in the duration of their crimes. The insiders who worked with outsiders perpetrated 69 percent of their crimes in a single operation; insiders who acted alone committed 56 percent in this way; and those who conspired with other insiders committed only 17 percent this way. Since crimes of extended duration involve long-term, periodic theft which exposes the insider to risk each time, it is reasonable that such operations would be unattractive to insiders who conspire with outsiders, if the payoff consists only of that which they have stolen. The insider would be doing all of the work, undergoing all of the risk, and still sharing the booty with an outsider. In only one insider/outsider case did this occur, i.e., that of the housekeeper who took dresses at the suggestion of the friend who acted as her fence.

When money is stolen instead of commodities and there is no need for a fence, which was the case in 72 percent of the insider/outsider incidents, crimes of extended duration become even more unlikely. The insiders who committed crimes of extended duration were either paid to do so (e.g., the weapons theft from the naval aviation depot) or the insider had essentially employed the outsiders (e.g., the drug smuggling ring managed by an airline agent).

Insiders who conspired with insiders committed crimes of extended duration 83 percent of the time. This would indicate that, on the whole, the attitude of insider conspirators toward their crimes differed from that of the insiders who worked with outsiders. Insiders who

---

House of Representatives, Subcommittee on Oversight and Evaluation, *U.S. Counterintelligence and Security Concerns: A Status Report, Personnel and Information Security,* Washington, D.C.: U.S. Government Printing Office, 1988.

amassed large quantities of loot by stealing small, unnoticeable portions at intervals were not willing to take large risks. An obvious crime involving a great deal of loot might force them to change their lives radically. These insiders, it seems, were usually interested in making some extra profit periodically, rather than masterminding a massive heist. Most insider conspirators probably considered the small amounts they stole to be their due. The crime, in fact, may have become simply another facet of their jobs—a second way to "earn" money. This surmise is somewhat substantiated by the insider conspirators' use of routine access in all cases.

## TACTICS AND LEVEL OF PLANNING

Theft or robbery, the crimes committed most often, comprised 71 percent of the incidents. Embezzlement was the second most frequent type of crime, accounting for 16 percent of the cases. Vandalism accounted for 5 percent, drug smuggling for another 5 percent, and the illegal communication of information for the remaining 3 percent. These figures basically correspond to those the Justice Department reported in 1985 regarding convictions in federal courts for white-collar and non-white-collar offenses.[3] The Justice Department found that 74 percent of those sentenced for federal offenses had committed non-white-collar crimes, and we found that 81 percent of the insiders in our sample committed such crimes. This similarity suggests that insiders, at least in their choice of crimes, are little different from the general criminal population.

Money was stolen in 60 percent of the incidents; however, insiders acting alone took money only 44 percent of the time, and insider conspirators took money only 50 percent of the time. The high incidence of thefts of money by insiders who worked with outsiders, 72 percent, accounts for the high overall total.

The incidents in which insiders worked with outsiders were carefully planned about 20 percent more often than those that involved the other two groups. Unlike the insider conspiracies, in which multiple participants were often necessary only for psychological support, insiders and outsiders who worked together usually needed each other either to perpetrate the crime or to make it profitable. The involvement of an outsider necessitated, in itself, a degree of planning. In some cases, insiders and outsiders had to search for appropriate partners; in three cases, insiders had to provide outsiders with disguises. While insider/

[3]U.S. Department of Justice, p. 6, Table 10.

outsider crimes were better planned than those of the other two categories, well-planned crimes were still the minority. Only 41 percent of the crimes perpetrated by insiders working with outsiders were well planned, as were only 29 percent of the crimes overall.

Crimes committed by insiders working with outsiders were also more inclined to be violent than were the others. Although only 23 percent of the insider crimes were violent, 31 percent of those committed by insiders working with outsiders involved violence (insiders in conspiracies used violence 17 percent of the time and lone insiders used violence in two cases). This difference in proportions cannot be attributed to the influence of the violent outsider, since in 50 percent of all violent crimes, the insiders themselves were violent. Insider and outsider groups' use of violence suggests, as does their careful planning, that they may have been more committed to their actions, for once they had used violence, there would be no way to hide the crime. Seventy-five percent of all violent crimes occurred at guarded targets, which is not surprising, since it is more likely that violence would be necessary for the crime to succeed when security is strong. Guarded targets would also be likely to be those of greatest value, which helps to explain the disproportionate use of force by the insiders and outsiders, the group whose thefts were of most value.

## SECURITY MEASURES AND PROCEDURES

As the small incidence of careful planning and violence indicates, the success of the majority of the insider crimes depended upon the perpetrators' exploitation of security deficiencies, including inadequate screening and supervision, failure to perform audits, and entrusting individuals with sole responsibility for the safety of valuables. In 33 percent of the incidents perpetrated by insiders and outsiders and in 7 percent of those perpetrated by lone insiders, the companies did not follow their own established security procedures, and this negligence contributed to the success of the crime. Since the insider conspirators were often the people responsible for enforcing security procedures, it is not surprising that 78 percent of the companies that suffered insider conspiracy crimes failed to practice the security measures they advocated. In 61 percent of the cases, security procedures were deficient in ways that allowed the insider to perpetrate the crime.

All three groups of insiders took advantage of security deficiencies in at least half of their crimes, but insiders working with outsiders, the group that planned extensively and used violence more often than any other, depended less upon security deficiencies than did the insiders in

the other two categories. Only 53 percent of those companies violated by insiders acting with outsiders suffered from a security deficiency that contributed to the success of the crime. In 47 percent of the cases in which insiders working with outsiders did exploit a security deficiency, this advantage was employed as only one part of their plan of operation. Insider conspirators utilized security deficiencies in 75 percent of their cases, and lone insiders in 83 percent.

As shown in Table 9, more than one deficiency frequently contributed to the success of the crime. Overall, lack of supervision ranked the highest: Lax supervision accounted for 34 percent of the total successful crimes. Problems with auditing ranked second, at 16 percent, while employee verification was the deficiency utilized the least.

**Table 9**

**DISTRIBUTION OF SECURITY DEFICIENCIES THAT CONTRIBUTED TO THE SUCCESS OF CRIMES**

| | Number of Crimes | | | | |
|---|---|---|---|---|---|
| Security Deficiency | Insider/ Outsider | Insider Conspiracy | Lone Insider | Total | Percent[a] |
| Supervision | 6 | 9 | 12 | 21 | 34 |
| Auditing | 3 | 2 | 5 | 10 | 16 |
| Shared responsibility | 5 | 2 | 1 | 8 | 13 |
| Off-site alarms | 5 | 0 | 3 | 8 | 13 |
| Prohibited areas | 3 | 0 | 2 | 5 | 8 |
| Employee verification | 3 | 0 | 0 | 3 | 5 |
| Total number of cases[b] | 17 | 9 | 12 | 38 | — |

[a]Percentages based on 62 total cases.

[b]In many cases, multiple deficiencies contributed to the success of a crime, so the individual deficiencies for each group do not add to the total number of cases aided by security deficiencies.

# IV. CONCLUSION

The insider criminal is among the most difficult and dangerous of adversaries to identify and to defend against. He or she may be young or old, a long-time or short-time employee. Although financial gain may be the insider's predominant motivation, additional elements such as family ties, intimate relationships, disillusionment or disgruntlement, misplaced altruism, or ideological allegiances may play a role in the decision to commit or abet a criminal act against an employer. Insiders can accomplish great damage acting either alone, in cooperation with fellow insiders, or in league with outsiders.

When we divided our database into three groups, we hypothesized that insiders who worked with outsiders would pose the most likely threat to a nuclear facility, because the difficulties and dangers involved in the theft of strategic nuclear material would demand the skills of a team of highly motivated individuals, coupled with the knowledge and access of an insider.[1] This is not to suggest that the threat posed by multiple insiders or the lone insider is negligible. The insider, driven by a psychological or emotional disturbance, could steal nuclear material or cause significant destruction to a nuclear facility entirely on his or her own. By the same token, a conspiratorial group of insiders could more easily steal nuclear material with the intention of later finding a buyer or undertaking a blackmail scheme. However, this study supports our hypothesis by revealing that crimes committed by insiders working with outsiders display more of the characteristics associated with a hypothetical nuclear crime than do those committed by the other two groups. Specifically, insiders who worked with outsiders created opportunities for crime using well-laid plans and incorporating associates they had sought, or who had sought them.

But, if an insider is most likely to commit a nuclear crime for, or in the company of, outsiders, how would the conspirators meet? In most of the insider/outsider cases, outsiders had established a relationship before they or the insiders spawned the idea for the crime. This is true even in cases involving ideological groups. The two insiders involved in the armored-car company theft perpetrated for the Order were both members of a white supremacist group before they suggested the crime. The Social Security embezzler, who was accused of following the orders of a religious sect, was stealing money for her husband, the leader of

[1]Serious damage to a nuclear facility arising from vandalism or sabotage could, of course, be accomplished by each category of insider.

that sect; the woman who gave information to the Aryan Brotherhood did so at the instigation of her boyfriend, a member of the gang; and the guard at the armored-car depot who stole millions for *Los Macheteros* was the son of a long-time Puerto Rican *independista* activist. Certainly, a sympathizer, an individual with close personal links, or even a covert operative of a terrorist group might be employed at a nuclear facility as well, unless a background check discovered that association.

While the incidence of preestablished relationships between ideological groups and insiders seems high, it would of course drop drastically if one considered only the coincidental relationships between employees of nuclear facilities and such groups. Nevertheless, the chance does exist; and if such a relationship were to occur, the motivations for the insider to commit the crime would increase because of personal loyalties. It is also entirely conceivable that an outsider might deliberately cultivate a friendship or an intimate relationship with an employee in order to eventually persuade or pressure that employee either to perpetrate some crime, assist in its commission, or furnish crucial information. Based on our findings, it is also possible that a coincidental connection between an employee at a nuclear facility and a political group would provide one or the other with the very inspiration for the crime.

If no prior relationship exists, either an insider eager to sell access, information, or stolen strategic nuclear material would have to find a buyer, or an outside group that desires such services or goods would have to locate an insider willing to betray both his or her country and employer to sell them. Our database includes two examples of insiders approaching outsiders and two examples of outsiders approaching insiders, all of whom were previously unknown to each other. The guard at the electronics warehouse and the cargo agent for the international airline both managed, by tapping into the criminal underground, to contact persons who were willing to pay for their help. The success of an employee of a nuclear facility in contacting a political group interested in his or her wares would, of course, depend upon the accessibility of such a group. The cases in which outsiders approached insiders include one in which the head of a drug-smuggling ring recruited bank tellers to launder his money and one in which a crime ring commissioned an insider to steal aircraft parts from a naval aviation depot to sell to Iran. The latter is frighteningly analogous to a situation that might occur at a nuclear facility.

If a hostile group located an employee who could supply them with crucial information or access or who could even steal the nuclear material for them, it might attempt to coerce that person by

threatening him or his family. Neither coercion nor time-consuming infiltration, however, appears to be as likely a means of co-opting insiders as simple bribery. According to the evidence gleaned from this study, financial gain was the factor most likely to motivate an insider to help outsiders perpetrate a crime. As discussed above, even those insiders who assisted ideological groups did so partly to reap monetary and emotional rewards.

It should be noted, however, that the main difference between the types of conventional crime examined in this report and a potential nuclear crime is the probable presence of ideology as the primary motivating factor in the latter. The ideologically motivated insider who wants to commit sabotage (with or without human victims) is entirely in the service of his ideology, and motivations such as financial gain, mental instability, or job disillusionment would have no bearing. The insider and outsider may have rather different motives for the commission of a nuclear crime. The outsider may want to steal nuclear material either for blackmail or actual use by himself or a foreign government or he may be intent on sabotaging or destroying the nuclear facility itself. The insider could have entirely different motives, e.g., he might be driven by financial gain when ideologically motivated outsiders offer him money for information or for assisting in the commission of a crime.

Moreover, ideologically motivated groups who might want to cause damage (sabotage the facility, release radioactive elements into the air, or even cause a meltdown of a reactor) would also want a large publicity payoff, whereas all the crimes for financial gain described in this report were strictly between perpetrator and victim. Further, in almost all of the incidents we examined,[2] the perpetrator's main desire was to keep his or her act from becoming known, in contrast to the attention-garnering act that an ideological adversary might seek to perpetrate against a nuclear facility. For this reason, the reliance on analogs in this report, although useful in identifying important indicators of *conventional* (i.e., nonnuclear) insider crime, can result only in hypothetical extrapolation.

Perhaps the most important findings of this study are those related to planning and security. In most of the crimes examined here, success seemed to depend less on detailed planning or expert execution than on the exploitation of existing security flaws. Indeed, most of these crimes did not require much planning at all, but rather took advantage of targets of opportunity. As an airline security official noted in the

[2]The vandalizing of fuel at a nuclear powerplant by two employees to call attention to defective safeguards practices was the exception.

NRC report, most high-value losses are not system failures, but people failures.

Guard forces present a special and particularly vexing problem. Guards were responsible for 41 percent of the crimes committed *against guarded targets.* Thus, the security routines themselves are not necessarily wanting; rather, they are often not properly followed. This problem might be alleviated by providing guards with some positive motivation, e.g., rotation from monotonous routines, higher pay, or other incentives, that could instill a long-term commitment to their jobs and employers. The problem of poorly motivated guards becomes even more serious in the setting of nuclear powerplants or nuclear weapons facilities that are protected by contract guard forces. The finding that nearly half of the crimes committed at guarded targets were abetted or executed by those charged with guarding those targets is an important reminder of the importance of encouraging greater reliability in a guard force.

In sum, no organization, no matter how ingeniously protected, can operate without some trust in individuals on all levels. Beyond a certain point, security considerations in hiring, guarding, controlling, and checking people can become so cumbersome as to actually impede the operation of a facility. This creates a serious dilemma in the case of a nuclear facility, where one accident or one successful crime is one too many. Society can generally absorb and recover from a bank robbery, a jewel theft, or the vandalizing of a factory or business. But the social and political—as well as the physical—fallout from a nuclear crime is such that adequate, or even very good, protection is not enough. On the other hand, total security can never be attained. Nevertheless, security officials can and must keep all possibilities of insider crimes in mind at all times, so that they can avoid surprises and be prepared at least for damage minimization, if damage prevention fails.

# Appendix A

# INCIDENTS IN THE INSIDER CRIME DATABASE

## INSIDER/OUTSIDER CRIMES

- A woman in charge of authorizing social security benefits obtained more than $500,000 by manipulating computer accounts to "create" dependent children whose benefits were paid to her under a false identity. She also fabricated credit histories that she and her brother used to cash fraudulent checks.
- After a television announcer had enlisted friends to purchase huge quantities of lottery tickets, he and a stagehand, a set designer, and a lottery official rigged one night's drawing. They filled specific ping pong balls with liquid so that the numbers they had chosen would be lighter, causing them to stay on top and win $1.2 million.
- A bank employee in Vancouver who had access to the code that allowed wire transfers of funds attempted to send $2.8 million to an accomplice at another bank in Los Angeles.
- Two members of a white supremacist group, the Order, furnished information to help the group steal $3.6 million from the armored-car company where they were supervisors. The insiders also initiated plans for a second heist, for which they provided the Order with maps and sketches of the company's central vault.
- A cargo agent at an international airline plotted a robbery of $5 million in cash and nearly $1 million in jewels with a second employee who later backed out and was paid $10,000 to keep quiet. The agent, whose job was to authorize transports of cash, left his post for one and a half hours, ensuring that the driver of an armored truck who was supposed to pick up a shipment of valuables would be unable to obtain his signature and would therefore leave the shipment at the airport. At 3:00 the next morning, the agent's accomplices pounced, bound and gagged airline employees, and made off with the loot. It is suspected that the thieves may have paid an organized crime syndicate for permission to execute this heist.

- A former employee of an armored-car company tricked a guard into opening a door and then rushed in with a ski-masked accomplice, tying up the guards and taking $7 million.
- A guard invited the leader of a crime ring to steal $2.7 million worth of computer microchips while the guard was on duty at an electronics company warehouse.
- An employee responsible for ordering and moving aircraft parts at a U.S. naval aviation depot stole one part every two weeks for several years for a criminal organization, which then sold the parts to Iran.
- In the nation's largest bank embezzlement case, a loan officer took $21.3 million over a period of four years by covering bad checks for the president of a sports promotion company.
- The central vault manager at a bank in Nevada stole $2.7 million by pretending to lock the bank's doors and then returning late at night with two accomplices to empty the vault.
- Four friends wearing business suits and carrying guns executed a plan masterminded by the assistant head teller at a New York bank who was also the lover of one of the four. One of the men inquired about renting a safe deposit box and then held up a guard in the vault. His three accomplices took the cash that employees had been counting for the tellers.
- Two brothers, one of whom was a cargo handler, stowed away in an airliner's baggage compartment that contained $2 million in securities. When the plane landed in Los Angeles, the two men absconded with the securities. Two other men were also involved in this plot.
- Two friends of a teller at a Los Angeles bank pretended to force him at gunpoint to open the vault, then "kidnapped" him along with money they took from other tellers.
- A cocaine kingpin paid two bank employees in Florida to launder approximately $55 million.
- New York City detectives foiled an employee of an armored-car company and two accomplices as they attempted to steal more than $1.2 billion in stock certificates from an armored car as it made its delivery.
- A security guard at an armored-car company in Chicago persuaded the two employees on duty with him to leave the premises so that he would be alone when six accomplices arrived; he entered the vault with the accomplices and escaped with $4.3 million.

- The secretary to a vice president of a New York bank transferred $100,000 to the account of a friend and $1 million to the account of a diamond dealer from whom he purchased at least nine diamonds.
- A part-time postal carrier asked two friends to waylay her truck while she was making her downtown Los Angeles jewelry mart run. They took $1.8 million in jewels and furs.
- A mechanic who worked on automated mail-sorting equipment stole $1.3 million in state refund checks, U.S. Treasury checks, and commercial checks. He turned the checks over to accomplices who sold them at less than face value to others who, in turn, deposited them in bank accounts bearing fictitious names.
- Five friends planned and executed the robbery of $11 million from an armored-car company where one of them worked as a guard. The guard claimed he had been surprised by gunmen while he was watching television in the company warehouse. The guard's father was also arrested for helping to hide some of the loot. The thieves reportedly paid organized crime for protection.
- An employee at a Tennessee bank supplied her accomplices with maps, keys, and uniforms as part of a plot to steal $6.5 million. She was found bound and gagged after the "robbers" had apparently broken into her office.
- A messenger on Wall Street was arrested along with his girlfriend's father in connection with the theft of $4 million in negotiable bank certificates. He had claimed that the certificates had been stolen from him as he was transporting them from a bank to his employer's offices.
- A program technician at the California State Franchise Tax Board obtained the home addresses of prison guards for the Aryan Brotherhood, the national white supremacist prison gang of which her boyfriend was a member. The group had targeted the guards for assassination.
- A security guard for an armored-car company, who had been employed for only two weeks, disappeared with $200,000 he had collected from an Arizona restaurant. An accomplice with a car facilitated the guard's escape.
- An armored-car guard, at the behest of the Puerto Rican terrorist group *Los Macheteros*, tied up two co-workers and made off with $7 million.
- A passenger agent for an international airline arranged to have tons of cocaine smuggled aboard U.S.-bound planes by service agents in Brazil. He then used his connection with the airline

to circumvent Customs agents. He also flew couriers to Brazil and erased the records of their trips. Three other passenger agents were involved in this scheme as well.

- Eight skycaps helped smuggle narcotics into Miami by routing baggage to two Customs inspectors who had been bribed to ignore the drugs.
- A guard who worked for an armored-car company at a New York location arrived one morning at a different location and convinced the other employees that he was supposed to work there for the day. After working for two hours, he grabbed a shotgun and handcuffed two workers. He and an accomplice whom he had disguised as an employee then walked out with several bags of cash.
- A housekeeper at a large department store stole 343 dresses at the rate of about 4 per week and sold them to an accomplice.
- A head cashier embezzled $1.5 million from a state treasury over a period of several years. She prevented her actions from being discovered by transferring anyone who began to find out too much about the way operations were run in her department. Later, she could not remember having committed the crime, and doctors diagnosed hysterical amnesia, a condition in which an entire life period is forgotten. The money was used to aid the career of a bandleader with whom the cashier was intimately involved.
- A guard with two accomplices stole historical objects from a museum to raise money to buy drugs.

## INSIDER CONSPIRACIES

- At least 50 U.S. Marines stole an estimated $500,000 worth of military equipment, which they then sold to surplus stores.
- Seven armored car guards employed by a private security company that had been hired by a major U.S. city to collect revenue from parking meters systematically stole more than $3 million in coins from the meters over a two-year period.
- Eleven of 16 employees in the coin department of a Federal Reserve Bank branch were part of an organized ring that stole more than $60,000 in coins and currency over a two-year period.
- Twenty-two baggage handlers employed by a major U.S. airline were involved in smuggling cocaine on board aircraft from

Colombia to Miami. An average of 300 pounds of cocaine was smuggled on a weekly basis.

- Active and reserve-duty personnel stole military equipment (including land mines and other weapons) from U.S. Army and National Guard bases in North Carolina and sold the equipment to the White Patriot Party, an extremist white supremacist organization.
- A father and son employed by an armored-car company robbed one of the company's armored cars at gunpoint. The father, who had recently been promoted to a supervisory post, had arranged for his son, a former convict, to be hired by the company. While the son and his partner were sitting in the armored car at a shopping mall, the father arrived and—through his supervisory capacity—gained entrance to the car. He and his son then overpowered the other guard and escaped with the money that was being transported in the armored car.
- Five sanitation workers stole $150,000 worth of postage stamps that were supposed to have been destroyed and sold them to a discount stamp dealer.
- Two employees of a commercial nuclear powerplant who had both previously served on U.S. Navy nuclear-powered vessels vandalized fuel at the facility. Their experience in the Navy had caused them to believe that the security and safeguards standards at the powerplant were inadequate. They therefore decided to call attention to the situation by vandalizing the fuel and then holding a press conference.
- A U.S. postal clerk and an accomplice stole jewelry from parcels sent by a specific business concern over a two-year period.
- The head supervisor of window clerks at a U.S. Post Office branch entered into a conspiracy with the clerks he was meant to be supervising whereby he would overlook window cash shortages. The clerks' end-of-day tallies would be signed by the supervisor as correct, indicating that all money was properly accounted for (when it was not). A total of eight employees were involved in the scam, which netted $104,500.
- A husband and wife who were joint managers of a U.S. postal contract station embezzled approximately $150,000 worth of postal money orders over a one-month period before being caught.
- Four cargo handlers employed by a major U.S. airline stole more than $1 million of merchandise and travelers checks from U.S. mail in transit at the airport. The thefts took place over a four-year period.

## LONE INSIDER CRIMES

- A taped telephone conversation revealed that an Army lieutenant planned to steal arms from Fort Myer and sell them to the Irish Republican Army.
- Over a period of two months, a clerk took $1.5 million worth of gold South African coins from the armored-car company at which he worked.
- While his partner was busy away from their truck, a guard drove off with the $1.85 million that he was supposed to be protecting.
- A former telephone company salesman illegally sold long-distance access codes to executives because he believed he had been unfairly deprived of commissions.
- A bank employee responsible for paying the bank's bills wrote debit tickets for more than the amount owed and pocketed the difference.
- A bank manager who believed he was dying of AIDS embezzled $1.1 million over a six-month period by establishing accounts under false names and transferring money into them. He donated some of the money to a home for AIDS victims, gave some to friends, and bought a house for himself.
- A computer-programming consultant at a bank in California easily located the daily code for wiring money, called the bank pretending to be an officer, and transferred $10.25 million to his own account in New York. With the money, he purchased diamonds in Switzerland, completing a deal he had previously arranged, and smuggled the jewels into the United States. He than opened a brokerage firm in New York through which he intended to sell the stones.
- An armored-car driver collected six bags of money from various branches of a bank in New Jersey, but delivered only three, keeping $370,000 for himself. He disappeared soon afterward.
- When two armored-car guards returned from a coffee break, they discovered a note from a third guard whom they had left to watch $1.5 million. "I have left with the money," the note read, "Don't call the police. Give me time to get away."
- An employee who worked as an operating and maintenance mechanic at a commercial nuclear plant set fire to a wooden shack in an auxiliary building located about 100 feet from the main reactor.
- An employee responsible for computer security at a Texas corporation introduced a virus into the computer system. The

virus activated two days after the employee was fired and wiped out 68,000 payroll records.

- In the first of four postal employee crimes, a man who had worked in the post office for 20 years stole stamps that were to have been destroyed and sold them to a discount dealer. In the second crime, a clerk took $100,000 from the cash drawer over a 10-year period. The third crime involved a carrier who stole registered mail packages that he correctly guessed to contain jewelry. A clerk in the fourth crime twice took the post office's bank deposit.
- A packing and shipping clerk entered a locked storage room at an art museum and made off with $3 million worth of Cezanne paintings. He quit his job shortly after being questioned about the robbery. Later, he contacted museum officials, telling them that the thieves had asked him to exchange the paintings for $250,000.
- A chief of security at a museum left work one day with Monet paintings valued at $1 million. He initially planned to replace the paintings with fakes but damaged the frames while removing the originals. Claiming that he had talked the thieves into returning the paintings, he brought them back frameless.
- A security guard at a museum stole gold coins, jewelry, and decorative objects from a storage locker where they were being kept during the building's renovation.

# Appendix B

# CHANGES IN SECURITY PROCEDURES RESULTING FROM INSIDER CRIME

## INSIDER/OUTSIDER CRIMES

- The machines for the lottery that was victimized are now always within the sight of lottery officials and video cameras. A lottery official, a group of senior citizens, and a CPA are present at all drawings, and the balls are now weighed both before and after they are chosen.
- An electronics company now ensures that its guards never work alone. It also monitors offsite alarms.
- The aviation depot increased supervision and separated tasks to reduce employees' control of specific aircraft parts. It also improved its audit trails and now trusts the checking of transactions to a computer rather than to a human.
- One bank from which a loan officer embezzled money for several years has speeded the process of checking debits and credits by five days, to monitor branch settlements more closely. It also sends out tracers when debits and credits do not match.
- Another bank has begun setting a 24-hour guard and has tripled its closed-circuit television since a supervisor broke into the vault late one night. During the day, a vice-president now closely oversees the operations once carried out by the thieving employee.
- Skycaps who once bribed Customs officials to facilitate smuggling may now assist passengers only after they have cleared Customs.
- The armored-car company that was robbed by men who misrepresented themselves as employees has added a supervisor to every tour of duty, requires that employees carry numbered identification cards, and has adopted elaborate verification procedures to ensure that people are who they claim to be.
- The state treasury from which a head cashier embezzled $1.5 million has divided up all of that individual's former tasks. It

has also consolidated its check-writing process and instigated surprise cash counts.
- The department store from which the housekeeper took dresses has increased its supervision over its staff and removed the doors from the housekeeper's supply rooms.

## INSIDER CONSPIRACIES

- On the recommendation of a Government Accounting Office study, security locks were installed at a Marine base from which military equipment was stolen (previously only padlocks were in place); warehouses were placed behind a fenced-in area; tighter inventory control was established so that every new supply officer conducted thorough inventories on a yearly basis. Now, more than one person must check out equipment and do so in the presence of a noncommissioned officer. Those who checked out the equipment are not allowed to be on duty when it is returned.
- Following the theft of coins and currency at a U.S. government storage facility, a new, slightly expanded background check was instituted and a different private security company was employed to administer it. A total surveillance system was put in place—including cameras, monitors, and taping equipment. This was done by the bank and not by a private security firm. It was designed to trace the flow of money and coins "from cradle to grave." Also, a metal detector was installed at entry/exit points. A library of tapes is maintained for 30 days, and the tape is recycled after that period. If an audit reveals a shortage, the tape is reviewed.
- A year before the baggage handlers were found smuggling narcotics, the Federal Aviation Administration had instituted a required five-year employment check (legally, however, a company cannot state why an employee left his or her job). This was of no assistance in preventing that particular crime. Prior security arrangements had called for the plane to land in Colombia and be searched and secured by guards, who would stay on it overnight. The aircraft would again be checked in the morning and then flown to the United States. One of the first changes after the incident was the firing of the private security guard company. Now guards are regularly rotated, so that none will be in the same position for more than a month.

- Although the nuclear powerplant that was vandalized did not make any changes in background screening procedures—since the two criminals had held the highest-level clearances while in the U.S. Navy and had been subjected to rigorous background checks—changes were made in internal security procedures. Closer supervisory attention was mandated, and managers and other persons in positions of responsibility received additional—and better—training in how to spot aberrant behavior. One respondent noted that the commercial nuclear industry was "at an infant stage in those days," but that security is much better now.
- A National Agency Check for fingerprints was instituted recently for employees of the U.S. Postal Service.

## LONE INSIDER CRIMES

- The bank from which the AIDS victim embezzled money has since changed its screening procedures. It now attempts to research applicants' credit history, honesty, drug use, and previous employers. The bank has also limited the hours in which transactions can be made involving the account from which the embezzler took money.
- After a computer programming consultant transferred $10.5 million from a bank into his own account, the bank completely overhauled its federal wire security system. The bank's security director will not divulge precisely what changes were made.
- One museum now runs a more thorough background check than before. The security department verifies lapses in residence and employment, investigates credit histories, and compares information the applicants volunteer with information they have given to former employers. Security directors at other museums and companies answer questions about former employees that cannot legally be asked, and the museum cultivates its connections with these security directors. It also depends upon the informal cooperation of the police to identify potential insiders; and supervisors have been instructed to observe lateness, unexplained absences, and employees borrowing money from each other.
- Another museum has stopped allowing employees to take keys home and has given master keys to only three people. Now, no one is allowed to work in the building at night, and no one may

ever be in the museum alone. The museum also added motion detectors and alarms that are monitored offsite.

- A third museum more than tripled its guard force, no longer uses guards from outside companies, and trains its guards thoroughly before they begin work. Rewards for seniority encourage long-term loyalty. The security staff alone is allowed in the building between midnight and 6 a.m., and nonsecurity employees who wish to work between 6 p.m. and midnight must have permission from their department head and the security director. All employees must carry identification cards, and these cards must be coupled with a key for an employee to enter a storage room. Three security control rooms of guards monitor all alarms and record who enters the storage rooms and when. Preemployment screening involves filling out double applications, completing an "honesty test," and submitting to a special investigations division that checks all civil, driving, and criminal records, the latter through informal relations with the police.

RAND/R-3782-DOE