116839

A STUDY OF TRADE SECRETS THEFT IN HIGH-TECHNOLOGY INDUSTRIES

by
Lois Felson Mock
National Institute of Justice
and
Dennis Rosenbaum
University of Illinois at Chicago

May, 1988

A STUDY OF TRADE SECRETS THEFT IN HIGH-TECHNOLOGY INDUSTRIES

by

Lois Felson Mock
National Institute of Justice

and

Dennis Rosenbaum
University of Illinois at Chicago

May, 1988

This project was supported by Purchase Order Number OJP-87-M235, awarded to the Center for Research in Law and Justice, University of Illinois at Chicago, by the National Institute of Justice, U.S. Department of Justice, under the Omnibus Crime Control and Safe Streets Act of 1968, as amended. Points of view or opinions expressed in this report are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

ACKNOWLEDGEMENTS

The Principal Investigators gratefully acknowledge the invaluable advice and assistance of the members of the project Advisory Board, without whom this study would never have been accomplished. They were instrumental in initiating the research, contributed their considerable expertise to the development of the survey instruments, and were responsible for making the "support calls" that were essential to the test of alternative survey methods.

As Directors of Corporate Security for major U.S. companies, the demands on their time and attention are very great and we appreciate the many hours they have devoted to this study and the unflagging interest they have shown in its effective execution.

Specifically, we wish to thank the following Advisory Board members:

Gerald Brandt
Helene Curtis, Inc.

Robert Burke
Monsanto Corporation

Dennis Dalton
Continental Bank

Richard Guilmette
Prime Computer, Inc.

Brian Hollstein
Xerox Corporation

Dillard Howell
Eli Lilly and Company

Raymond Humphrey
Digital Equipment Corporation

James Jessee
Proctor and Gamble

Robert Kitzinger
Ameritech Corporation

Richard Mainey
IBM Corporation

James Royer
FMC Corporation

Myron Weinstein
Texas Instruments

In addition to the Advisory Board, we also express our appreciation to Charles (Sandy) Davidson, Staff Director of the American Society for Industrial Security (ASIS) Foundation, Inc., for his facilitation of the ASIS Foundation grant award to the project, and to both Mr. Davidson and Paul Diderio, for providing the ASIS membership lists and mailing labels that were essential to the sampling and data collection activities.

TABLE OF CONTENTS

INTRODUCTION

Background of the Study

"Industrial espionage" -- the theft of proprietary information or trade secrets from U.S. industries -- is an economic and criminal justice problem of growing concern as a threat to the vitality of American companies, especially those engaged in the development, manufacture, and sale of high technology equipment. The current level of knowledge about the nature and extent of trade secrets theft and about existing company procedures for its prevention and control, however, remains extremely limited.

Because of their concern, security directors representing the High Technology Division of the American Society for Industrial Security (ASIS) approached the National Institute of Justice (NIJ) to discuss the need for a national survey of trade secrets theft that would provide an empirical basis for assessing the problem and for developing more effective legislative, criminal justice, and company remedies to it.

While agreeing on the need for research to address the theft of trade secrets in high-technology industries, participants in these discussions recognized that the conduct of a large-scale national survey would be premature without the prior resolution of three important methodological issues.

First, because of the lack of previous empirical research, there was a need to ascertain whether security directors would admit that their companies had been victims of trade secrets theft and, if so, whether victimization was extensive enough in high-technology companies to merit a large-scale national study.

Second, because trade secrets theft might be considered a "sensitive issue" by many high-technology companies, some industry respondents might be reluctant to participate in a survey on this subject. Therefore, exploratory research was necessary to determine the extent of the non-response problem (if any) and to identify those survey methods that would most effectively overcome it.

And finally, because of the complexity of the issues involved and the limited previous efforts to scientifically study them, considerable preparatory research was needed to identify what variables should be measured (what questions should be asked) in the survey in order to collect the information necessary for a comprehensive exploration of the problem. Furthermore, the construction of a reliable survey instrument required an extensive development and pilot testing process prior to its use in a large-scale national study.

For these reasons, NIJ and ASIS decided to co-sponsor a small-scale preliminary survey on trade secrets theft which would both lay the groundwork for a more comprehensive national survey by resolving these important methodological concerns and, at the same time, would collect initial substantive data on the nature of the problem and company responses to it.

The study was a collaborative research effort by Lois Felson Mock, of the National Institute of Justice, and Dennis Rosenbaum, of the University of Illinois at Chicago. The two principal investigators were jointly responsible for the design of the study and, in collaboration with the project Advisory Board, for the development of the survey instruments, with Dennis Rosenbaum assuming primary responsibility for the survey administration and data preparation and Lois Mock assuming primary responsibility for the data analysis and research report.

What follows is a report which describes the study sample and research goals, discusses the examination and resolution of the methodological issues, and presents the substantive survey findings on trade secrets theft in high-technology companies.

Study Sample

The project sample was generated from the ASIS membership lists of "Directors of Security" in three types of industries: (a) Communications; (b) Oil, Gas, and Mining; and (c) Industrial and Manufacturing. These three categories were selected because they included the greatest number of "high-technology" companies and encompassed a wide range of companies reflecting a diversity of U.S. industries. However, while the companies included in these categories are located throughout the United States, the extent to which they are representative of large American high-technology companies in general is unknown, since not all security directors of such companies may be ASIS members and since there is no universally-accepted definition of "high technology".

Prioir to sample selection, the ASIS membership lists were "cleaned" to eliminate names defined as "ineligible" for the project sample for the following reasons: (1) the person listed was not clearly identifiable as responsible for company security (e.g., company president); (2) the person listed did not have a company affiliation; (3) the company was a vendor of security or related services; (4) the company was primarily a defense contractor; (5) the security director (company) was located outside of the United States; (6) the security director was a member of the project Advisory Board; or (7) the company was also included in the project's "Known Victim Sample" (described below). In addition, because the remaining number of "eligible" names was larger than the study sample required to ensure at least 100 survey respondents (completions), further names were randomly deleted, primarily from the "Industrial and Manufacturing" category, which was much larger than the other two industry types. [In all of the data tables and discussion, responses of security directors in each of the three categories have been weighted to make their representation in our sample equal to their representation in the ASIS membership population.]

Reflecting these deletions, the final sample selected to be surveyed included 41 "Communications" companies; 45 "Oil, Gas, and Mining" companies; and 124 "Industrial and Manufacturing" companies, for a total sample size of 210 companies.

Research Goals

I. To lay the methodological groundwork for a potential national survey on the theft of trade secrets in high-technology industries.

A. To determine the feasibility of conducting a large-scale national survey by testing:

1. Whether high-technology companies will admit to trade secret theft victimization.

2. Whether victimization is extensive enough to warrant a comprehensive national study.

B. To test the relative effectiveness of the following alternative survey methodologies for maximizing the response rate of security directors to the survey:

1. Mail Survey versus Telephone Survey, both accompanied by a letter of support from the President of ASIS.

2. Prior Support Call versus No Support Call from a "respected colleague" (fellow ASIS security director).

C. To develop and pilot test a survey instrument (questionnaire) which will effectively measure those variables critical to an understanding of trade secrets theft and its prevention and control.

II. To collect substantive data on the theft of trade secrets in high-technology industries.

To collect information on high-technology companies; on their trade secrets theft incidents; on company and criminal justice responses to these offenses; and on security director attitudes about the problem.

I. METHODOLOGICAL FINDINGS

Part I of this report addresses Goal I of the study, as detailed in the previous section, and presents findings relating to the conduct of a potential national survey on trade secrets theft. Results are discussed in three sections, corresponding to the three methodological subgoals, which deal, respectively, with: (A) National Survey Feasibility; (B) Response Rates to Alternative Survey Methods; and (C) Development and Pilot Testing of the Questionnaire.

A. National Survey Feasibility

Admission of Victimization

To test whether security directors would admit that their companies had been victims of trade secrets theft, the study added to its primary ASIS membership sample a sample of 29 "known victim" companies identified from newspaper articles, input from security directors, and computer listings of court cases in the last ten years. When asked "Has your company ever experienced a theft of trade secrets?", the responses of the 17 "known victims" who completed the survey were as follows:

	Percent
Yes	76.5
No	17.6
No Answer	5.9
	(N= 17)

As these findings show, more than three fourths of the victims did admit their victimizations, while only three of them (18%) actually denied the thefts. Responses of the larger ASIS membership sample, reported in the following section, corroborate these "known victim" sample findings, also showing that a substantial percentage of security directors are willing to admit company victimizations.

Extent of Victimization

To determine the extent of trade secrets theft in high-technology companies in general, the ASIS membership sample was asked a series of victimization questions. When asked "Has your company ever experienced a theft of trade secrets?", the 150 security directors who responded to the survey reported their victimization as presented below.

	Percent
Yes	48.0
No	36.7
Don't Know/No Answer	15.3
	(N=150)

As the table shows, almost half of the respondents said that their companies had been the victims of trade secret theft, while only about a third indicated that they had not been victimized.

In addition, to find out the recency and frequency of these thefts, the 72 victimized respondents were asked about their incidents "in the last ten years" and "in the last five years" (see Table B2 in Part II of this report). Responses indicated that most of these companies had been victimized recently. Almost all (92%) had experienced thefts in the last ten years and 83 percent reported incidents in the last five years. Moreover, a majority of these companies had been multiple victims. More than half said that they had experienced at least two thefts during the last five years and more than twelve percent reported more than five.

Conclusion

These findings on the extent and admission of victimization show (a) that theft of trade secrets is quite prevalent in diverse types of large American high-technology companies and (b) that these companies are willing to report such thefts when responding to survey research. Therefore, with respect to these two critical issues, the data suggest that a comprehensive national survey of trade secrets theft would be feasible to conduct, at least for the types of companies included in this initial study.

B. Response Rates to Alternative Survey Methods

Mail Survey versus Telephone Survey

To test the relative effectiveness of mail versus telephone surveys in maximizing response rates, the 210 security directors in the ASIS membership sample were randomly assigned to one of these two methods and their rates of survey completion were compared. To ensure that at least 50 surveys would be completed in each method group, a larger proportion of the sample was assigned to receive a mail survey, since mail survey response rates are generally lower than response rates for telephone surveys. Thus, 130 security directors were scheduled to receive mail surveys and 80 were scheduled for telephone surveys. The following table compares the response rates for the two survey methods.

Survey Method	# Assigned	# Completed	Response Rate
Mail	130	90	69.2%
Telephone	80	60	75.0%

As the table shows, the response rates to both survey methods were greater than expected, especially for the mail survey. Thus, instead of 50 respondents in each of the two survey groups, 90 mail and 60 telephone surveys were completed, for a total of 150 respondents. As expected, the telephone survey method resulted in a higher response rate (75%) than the mail survey method (69%). However, this difference was not great (only 6%) and was smaller than the differences normally found between mail and telephone survey response rates.

Support Call versus No Support Call

Even though both mail and telephone surveys were accompanied by a support letter from the ASIS President, it was felt that additional encouragement might be required to convince security directors to participate, given the sensitive nature of the issues being addressed. To determine whether this was true, half of the mail and half of the telephone survey samples (a total of 105 security directors) were randomly assigned to receive the additional encouragement of a support call from a respected colleague in the security field, while the other half of each sample received no such call. The response rates of the "call" versus "no call" groups were then compared. The findings are shown below.

Survey Method	# Assigned	# Completed	Response Rate
Call	105	81	77.1%
No Call	105	69	65.7%

As the table shows, receiving a support call from a fellow ASIS security director increased the survey response rate, with 77 percent of the called sample completing their surveys, as compared with only 66 percent of those not receiving a call. Moreover, the response rate difference between these two groups (more than 11%) was almost twice as great as the difference between the mail and telephone survey groups.

Interaction Between Type Survey Call/No Call

When response rates for the four "combined-method" alternatives (mail/call, mail/no call, telephone/call, telephone/no call) were compared, an "interaction" effect was found. Therefore, while the previous results seem to attribute special importance to receiving a support call, this was not always true. As the following table illustrates, although support calls led to a substantial increase (of over 15%) in the response rate of mail survey respondents, they had almost no effect (only 3%) on the response rate of telephone survey respondents. That is, the

telephone survey methodology was able to achieve consistently high response rates with or without the addition of support calls, while the mail survey required a support call to achieve the same level of response.

Survey Method	# Assigned	# Completed	Response Rate
Mail			
Call	65	50	76.9%
No Call	65	40	61.5%
	Response Rate Difference =		15.4%
Telephone			
Call	40	31	77.5%
No Call	40	29	72.5%
	Response Rate Difference =		3.0%

Conclusion

Based on the response rate findings presented above, it can be concluded that three of the four alternative methods tested could be used to maximize response rate levels in a national survey of trade secrets theft: a mail survey accompanied by a support call from a respected security director colleague or telephone surveys with or without such a call. The one alternative to be avoided is a mail survey with no support call, which had a substantially lower response rate.

Since other considerations (such as quality of responses and survey costs) should also influence the selection of a survey method, the three "acceptable response rate" alternatives were further compared on these other selection factors. Study findings showed (a) that survey responses were somewhat more complete (i.e., more questions were appropriately answered) in the telephone survey than in the mail survey and (b) that the additional procedure of administering support calls added to the time and complexity of the data collection process, even for this small initial study sample, and could be expected to be much more difficult, time-consuming, and costly to implement in a large-scale national survey. Thus, it would appear that the most efficient and effective survey methodology for a future national study would be a telephone survey, preceded by a support letter from the President of ASIS (or other respected security professional), but without a support call from such a colleague.

C. Development and Pilot Testing of the Questionnaire

Questionnaire Development

Development of a survey instrument required the identification of the critical variables to be included on the survey. This was accomplished through the conduct of two "focus group" sessions, at which the project Advisory Board of Corporate Security Directors from major high-technology companies utilized their considerable expertise to inform the content and format of the questionnaire. Advisory Board members reviewed a draft survey instrument in detail and provided essential guidance for its revision and ultimate design.

Pilot Testing

Once finalized, the survey instrument was comprehensively tested on the study sample. Both mail and telephone surveys were successfully conducted, resulting in appropriate and informative responses from most respondents. As mentioned above, the telephone survey responses contained fewer unanswered items and fewer inappropriate answers, which was to be expected, given that an experienced interviewer guided these respondents through the questionnaire. However, interviewers identified a number of specific questions that should be improved if a national study were to be conducted.

Conclusion

Based on these findings, it is concluded that, with minimal improvements, the questionnaire developed and tested in this initial project could serve as an effective data collection instrument for a future national study utilizing either a mail or a telephone survey methodology.

II. SUBSTANTIVE FINDINGS ON TRADE SECRETS THEFT

Part II of this report addresses Goal II of the study, as specified in the introductory section on "Research Goals", and presents the substantive survey information collected on trade secrets theft. Descriptive findings for the survey items are reported in four sections, corresponding to the four sections in the questionnaire: (A) Background Information on High-Technology Companies; (B) Characteristics of Theft Incidents; (C) Responses to Theft Incidents; and (D) Opinions About Trade Secrets Theft. Each section includes a summary description of the more important findings for the section, followed by a set of tables detailing the responses to most of the individual questions in that section of the survey instrument.

A. Background Information on High-Technology Companies

Section A provides descriptive information about the companies in the survey sample. In general, these sample companies were very large. Their median number of employees (Table A2) was 3000 and more than one fourth of the sample employed 10,000 or more. Their 1986 gross income (Table A3) ranged from one million to thirty billion dollars, with 29 percent of the companies earning over one billion. Almost all of the sample were multi-office companies. Over 95 percent had offices in more than one city (Table A4), 84 percent had branches in more than one state (Table A5), and two thirds had offices in more than one country (Table A7). The companies were also well-established, having been in existence for an average of sixty years (Table A8).

Sample companies were also security-conscious. More than 60 percent of them currently had a program to protect against trade secrets theft (Table A12) and most of these programs were not new; over 70 percent of them had been in existence for at least four years and almost one third were more than ten years old (Table A13). Company security directors were very experienced, as well. Almost three fourths of them had had at least ten years of experience in the security field and over 40 percent had been in security for more than twenty years (Table A10).

Section A Tables*

Table A2. "How many people does your company employ?"

	Percent
Less than 1000	21.3
1000-1999	16.7
2000-4999	23.3
5000-9999	11.3
10,000-19,000	8.7
20,000-49,000	12.7
50,000 or more	5.3
No Answer	.7
	(N=150)

Median: 3000

Table A3. "What was your company's sales or gross income for 1986?"

	Percent
Under $100 million	16.0
$100-999 million	32.0
$1-4 billion	20.7
$5 billion or more	8.0
Don't Know/No Answer	23.3
	(N=150)

Median: $365 million

* In all Part II sections, table numbers correspond to the numbers of their respective questions in the survey instrument.

Table A4. "Does your company have offices in more than one city?"

	Percent
Yes	95.3
No	4.0
No Answer	.7
	(N=150)

Table A5-6. "Does your company have offices in more than one state?" "In how many states is your company located?"

	Percent
Yes	84.0
No	7.3
No Answer	8.7
	(N=150)

Mean Number of States: 17

Table A7. "Does your company have offices in other countries?"

	Percent
Yes	66.7
No	32.0
Don't Know	1.3
	(N=150)

Table A8. "How old is your company?"

	Percent
Under 20 years	15.3
20-49 years	28.0
50-99 years	28.7
100 years or more	24.7
Don't Know/No Answer	3.3
	(N=150)

Mean: 60 years

Table A9. "What is your title or position in the company?"

	Percent
Director of Security	78.7
Legal/Patent Counsel	0.0
Comptroller/Auditor	0.0
Other	21.3
	(N=150)

Table A10. "How long have you been involved in the security field?"

	Percent
Less Than 1 Year	1.3
1-5 Years	7.3
6-10 Years	17.3
11-20 Years	30.7
More Than 20 Years	43.3
	(N=150)

Table A11. "How long have you been with the company?"

	Percent
Less Than 1 Year	2.7
1-5 Years	32.7
6-10 Years	32.7
11-20 Years	19.3
More Than 20 Years	12.7
	(N=150)

Table A12. "Does your company currently have a program to protect against trade secret theft?"

	Percent
Yes	61.3
No	34.0
Don't Know/No Answer	4.7
	(N=150)

Table A13. "How long has your company had a program?"

	Percent
Less Than 1 Year	4.3
1-3 Years	19.6
4-6 Years	23.9
7-10 Years	14.1
More Than 10 Years	32.6
Don't Know/No Answer	5.4
	(N=150)

B. Characteristics of Theft Incidents

Section B provides information on the incidence and frequency of trade secret theft for all companies in the sample. Then, for companies which have been victimized in the last ten years, information is provided on their "most recent incident": the circumstances of the crime, the characteristics and methods of the offender(s), and the factors contributing to theft occurrence.

Findings show that theft victimization was very extensive among the large, high-technology companies surveyed. Of the 150 companies responding to the survey, 48 percent (72 companies) reported that they had been victims of trade secrets theft at some time in the past (Table B1). In addition, most of these victimized companies had experienced theft recently. More than 90 percent (66 companies) reported incidents in the last ten years (Table B2) and over 80 percent had been victims in the last five years (Table B3). Furthermore, a majority of the victimized companies had been victims more than once, even within the last five years. Over half reported at least two thefts during this period and over twelve percent had experienced more than five.

Of the 66 companies victimized during the last ten years, more than three fourths reported that their "most recent incident" had occurred in 1985 or later (Table B6). About 60 percent of these companies learned about the theft from an internal source (Table B7), most frequently a co-worker of the offender (Table B8), through the discovery of physical evidence or through witness observation (Table B9). For the 40 percent of the companies who learned about the theft from external sources, the informant was most often a competitor of the victim (Table B10). "Research and development data" was the type of information most frequently targeted for theft -- in almost half of the incidents --, while "new technology" was second, being targeted in 38 percent (Table B11). In over 60 percent of the incidents, respondents reported that the theft was actually completed, rather than only attempted (Table B15).

With respect to the offenders in these "most recent" theft incidents, insiders were involved in a large majority (almost 80%) of the crimes, either alone or with outsiders, while outsiders were involved alone in only 17 percent of the incidents (Table B17). Compatible with this predominance of insider involvement, offenders had legitimate access to the target information in two thirds of the thefts (Table B16), with "physical theft" and "misuse of authority of position" being the two most frequently used methods for obtaining the targeted secrets (Table B13).

Consistent with these methods and with the research and technology types of information most frequently targeted for theft, the "typical inside offender", as described by respondents, was a company employee who occupyied a "technical or scientific" position (Table B19) in the "engineering or research" department (Table B20). Typically, this inside offender had been with the company for one to five years (Table B18), but had financial problems and/or was leaving to start his own business or take a new job at the time the theft occurred (Table B21).

The "typical outside offender", as identified by respondents, was an employee of a competitor (Table B23) who had interacted with the company for one to five years (Table B22) and who was involved with an inside offender in perpetrating the theft (Table B17).

When asked to identify important contributing factors to the incident (Table B24), only three factors were rated as "very important" contributors by a majority of the respondents: "severe market competition", "offender greed", and "attractiveness of the target information". Three other factors -- "offender ambition", "weak [company] management controls", and "lack of professional ethics" -- received "very important" ratings by more than a third of the respondents.

Section B Tables

Table B1. "Has your company ever experienced a theft of trade secrets, whereby someone inside or outside your company stole proprietary information or attempted to steal such information?"

	Percent
Yes	48.0
No	36.7
Don't Know/No Answer	15.3
	(N=150)

Table B2. "How many incidents of trade secret theft (or attempted theft) has your company experienced in the past ten years?"

Table B3. "How many...in the past five years?"

	Table B2 (10 yrs) Percent*	Table B3 (5 yrs) Percent*
One	23.6	25.0
2-3	32.0	36.1
4-5	13.9	8.3
More Than 5	20.8	12.5
None/No Answer	9.7	18.1
	(N=72)	(N=72)

* Percents are based on those 72 respondents who said "Yes" when asked if their company had "ever experienced a theft of trade secrets" (see Table B1).

[TABLES B6 - B24, WHICH FOLLOW, AND TABLES C1 - C12, IN THE NEXT SECTION, PROVIDE INFORMATION ABOUT THE COMPANY'S "MOST RECENT INCIDENT" IN THE LAST TEN YEARS. OF THE 150 COMPANIES RESPONDING TO THE SURVEY, 66 REPORTED INCIDENTS IN THE LAST TEN YEARS. THEREFORE, UNLESS OTHERWISE NOTED, THE PERCENTAGES PRESENTED IN THESE "B" AND "C" TABLES ARE BASED ON THOSE 66 COMPANIES REPORTING A "MOST RECENT INCIDENT" DURING THIS PERIOD.]

Table B6. "When was this incident discovered?"

	Percent
Prior to 1985	19.7
1985 - 1988	77.3
Don't Know/No Answer	3.0
	(N=66)

Table B7. "Did your company first learn about the trade secret theft from internal or external sources?"

	Percent
Internal Sources	59.1
External Sources	40.9
	(N=66)

Table B8. "What internal source provided the first information about the incident?"

	Percent*
Security Department	5.1
Audit Department	7.7
Marketing Department	15.4
Personnel Department	2.6
Line Management	7.7
Senior Management	5.1
A Co-Worker	28.2
The Guilty Party	0.0
Other	28.2
	(N=39)

* Percents in Tables B8 and B9 are based on the 39 companies which first learned about the theft from "Internal Sources" (see Table B7).

Table B9. "By what means was the incident first discovered?"

	Percent
Physical Evidence	28.2
Exit Interview or Follow-up	7.7
Internal Audit/Financial Analysis	5.1
Internal Competitive Analysis	5.1
Supervisory Inspection/Control	7.7
Witness Observation	30.8
Another Investigation	0.0
Confession	0.0
Anonymous Internal Tip	5.1
Other	10.3
	(N=39)

Table B10. "What external source provided the first information about the incident?"

	Percent*
Law Enforcement	6.3
A Competitor	28.1
Contractor/Supplier	18.8
A Job Applicant	0.0
An Anonymous Tip	6.3
An External Audit	3.1
Other	37.5
	(N=32)

* Percents are based on those 32 companies which first learned about the theft from "External Sources" (see Table B7).

Table B11. "What type of information was the target of the theft?"

	Percent* "Yes"
Customer Lists	28.8
Aquisition/Merger Data	3.0
Research/Devel Data	48.5
New Technology	37.9
Personnel Data	6.0
Financial Data	21.2
Program Plans	24.2
Other	18.2
	(N=66)

* Percents do not sum to 100.0 because more than one answer could be given.

Table B13. "What methods were used to obtain (or attempt to obtain) the proprietary information?"

	Percent*
Misuse of Authority/Position	48.5
Physical Theft	43.9
Computer Penetration	24.2
False Statements or Claims	21.2
Subversion of Employee	18.2
False Documents/Authorization	16.7
"Head Hunting" Debriefing	4.5
Wire Tapping or Bugging	1.5
Other	13.6
Don't Know	1.5
	(N=66)

* Percents are ranked by frequency of mention and do not sum to 100.0 because more than one answer could be given.

Table B15. "Was this trade secret incident a completed or attempted theft?"

	Percent
Completed	60.6
Attempted	36.4
Don't Know	3.0
	(N=66)

Table B16. "Did the offender have legitimate access to the target information?"

	Percent
Yes	66.7
No	30.3
Don't Know	3.0
	(N=66)

B17. "Were the offenders insiders, outsiders, or both?"

	Percent
Insiders	43.9
Outsiders	16.7
Both	34.9
Don't Know	4.5
	(N=66)

Table B18. "How many years had the primary insider been with the company?"

	Percent*
Less Than 1 Year	3.8
1-5 Years	42.3
6-10 Years	32.7
More Than 10 Years	15.4
Don't Know	5.8
	(N=52)

* Percents in Tables B18 - B21 are based on those 52 companies whose incidents involved "Insiders" or "Both" insiders and outsiders (see Table B17).

Table B19. "What was the primary insider's position level in the company?"

	Percent
Blue Collar	5.8
Clerical	5.8
Technical/Scientific	40.4
Middle Management	26.9
Senior Management	15.4
Other	5.8
	(N=52)

Table B20. "Where did the primary insider work within the company?"

	Percent
Financial/Auditing	1.9
Computer Functions	5.8
Engineering/Research	46.2
Marketing	25.0
Personnel	0.0
Management/Policy Devel	3.8
Security	0.0
Other	17.3
	(N=52)

Table B21. "Did the primary inside offender have any of the following characteristics?"

	Percent*
Starting His/Her Own Business	34.6
Financial Problems	30.8
Leaving for a New Job	30.8
Recently Fired/Demoted	15.4
An Alcohol Problem	11.5
Falsified Background Information	11.5
Recently Hired	5.8
A Drug Problem	1.9
Prior Arrests	0.0
Other	11.5
	(N=52)

* Percents are ranked by frequency of mention and do not sum to 100.0 because more than one answer could be given.

Table B22. "About how many years had the primary outsider interacted with your company?"

	Percent*
Less Than 1 Year	20.6
1-5 Years	38.2
6-10 Years	2.9
More Than 10 Years	8.8
Don't Know	29.4
	(N=34)

* Percents in Tables B22 and B23 are based on those 34 companies whose incidents involved "Outsiders" or "Both" insiders and outsiders (see Table B17).

Table B23. "What was the primary outsider's relationship to your company?"

	Percent
Consultant	14.7
Supplier	8.8
Customer	11.8
Competitor	32.4
Other	29.4
Don't Know	2.9
	(N=34)

Table B24. "In your opinion, what were the most important factors that contributed to this theft incident?"*

	Percent "Very Important"
Severe Market Competition	53.0
Offender Greed	50.5
Attractiveness of Target Secrets	50.5
Offender Ambition	43.9
Weak Management Controls	39.4
Lack of Professional Ethics	39.4
Offender Financial Need	30.3
Inadequate Employee Education	25.8
Inadequate Security Procedures	22.7
	(N=66)

* Table B24 includes only those factors which were rated as "Very Important" by more than 20 percent of the respondents and as "Very" or "Somewhat Important" (as opposed to "Not Important") by more than 50 percent.

C. Responses to Theft Incidents

Section C describes company and criminal justice responses to the 66 "most recent incidents" of trade secret theft, including techniques of investigation; criminal prosecution procedures and outcomes; civil actions and outcomes; and administrative measures to sanction offenders and prevent future thefts.

With respect to investigative responses, internal company investigations were conducted in over 90 percent of the incidents (Table C1), with security department staff assuming primary responsibility in almost all of these (Table C2). In contrast, public law enforcement investigations were conducted in only 15 percent of the thefts and were always an addition to (rather than a substitute for) the company's own investigation (Table C1).

When security directors were asked what methods were used to investigate their most recent theft incidents (Table C3), "interviews" were by far the most frequently cited technique, being employed in over 95 percent of the investigations. Interviews were also considered the most effective investigative method, being rated as "very effective" in more than three fourths of the investigations in which they were used. Following "interviews" in frequency of use were "examining documents" (used in 53% of the investigations) and "confidential informants" (used in 47%), both of which techniques were also rated as "very effective" in a majority of their cases. Effectiveness did not always parallel frequency of use, however. For example, while "auditing financial reports" was another strategy employed in many (44%) of the investigations, it was rated as "very effective" in only one third of these and, although "monitoring/electronic surveillance" was selected as an investigative method for only about one fifth of the cases, it was considered "very effective" in well over half of them. The remaining two methods of investigation -- "polygraph exams" and "drug or other lab tests" -- were neither used nor rated as "very effective" in most cases.

"Administrative actions" were by far the most frequent actions taken in response to trade secrets theft (Table C4), occurring in over 70 percent of the incidents. In contrast, "criminal prosecutions" and "civil actions" were each pursued in less than one fifth of the cases. However, although infrequent, where criminal and civil actions were pursued, completed cases generally resulted in convictions or settlements in favor of the company and in monetary and/or other sanctions against the offender (Tables C6-C8 and C10-C11).

When respondents were asked what types of administrative measures were used to sanction company employees involved in their most recent theft (Table C12), almost 90 percent said that the offending employee(s) had been terminated. Property recovery or restitution was also demanded in a majority of the cases involving company employees.

While administrative sanctions were less often imposed against outside companies involved in thefts, the most frequently used measure was the suspension or termination of a contract, which occurred in over one third of the cases involving outside companies (Table C12)

In addition to these sanctioning responses, victimized companies also took preventive actions to avoid similar theft incidents in the future (Table C12). Most frequently cited as a preventive action was "tighter management controls", used by more than 95 percent of the companies which employed administrative measures, followed by "tighter security" (used by 75%) and "improved record keeping" (used by 68%). "Changes in employee training" and "improved auditing procedures" were also implemented by a majority of these companies. As might be expected, the types of preventive actions most frequently taken were generally directed at those company weaknesses most often mentioned as "very important factors" in contributing to theft occurrence (see Table B24).

Finally, all of the above administrative actions were considered as "especially effective" by at least two thirds of the respondents whose companies had taken them (Table C12).

Section C Tables

Table C1. "Who investigated this incident?"

	Percent
Inside Investigators	93.9
Public Law Enforcement	15.2
No One	4.5
No Answer	1.5
	(N=66)

Table C2. "Who participated in the internal investigation? Of those who participated, who had primary responsibility for the investigation?"

	Participated	Responsibility
	Percent*,**	Percent*
Security Department Staff	91.9	69.4
Legal Department Staff	69.4	11.3
Accounting/Auditing Staff	21.0	0.0
Top Management	74.2	12.9
Line Management	50.0	4.8
Private Attorney	8.1	0.0
Private Investigators	9.7	1.6
Other	11.3	0.0
	(N=62)	(N=62)

* Percents are based on those 62 incidents which were investigated by "Inside Investigators" (see Table C1).

** Percents do not sum to 100.0 because more than one answer could be given.

Table C3. "For each of the following methods of investigation, please indicate whether it was very effective, somewhat effective, not very effective, or was not used in this case."

	Used	Very Effective
	Percent*	Percent**
Interviews	95.2	76.3
Examining Documents	53.2	60.6
Confidential Informants	46.8	51.7
Auditing Financial Reports	43.5	33.3
Monitoring/Elec Surveillance	22.6	57.1
Polygraph Exams	4.8	0.0
Drug and Other Lab Tests	4.8	33.3
Other	3.2	0.0
	(N=62)	

* Percents are based on those 62 incidents which were investigated by "Inside Investigators" (see Table C1).

** The percent for each method of investigation is based on the number of incidents in which this method was used, ranging from 2 incidents (for "Other") to 59 incidents (for "Interviews").

Table C4. "Which of the following actions were taken [in response to the most recent theft incident]?"

	Percent* "Yes"
Referral for Criminal Prosecution	18.2
Referral for Civil Action	16.7
Administrative Action(s)	71.2
Other Action	3.0
No Further Actions	12.1
	(N=66)

* Percents do not sum to 100.0 because more than one answer could be given.

Table C5. "To whom was the case referred for criminal prosecution?"

	Percent*
U.S.Attorney	16.7
District Attorney	58.3
Don't Know/No Answer	25.0
	(N=12)

* Percents for Tables C5 and C6 are based on those 12 cases referred for Criminal Prosecution (see Table C4).

Table C6. "Were any criminal charges filed?"

	Percent
Yes	66.7
No	33.3
	(N=12)

Table C7. "Were there any guilty pleas or convictions at trial?"

	Percent*
Yes, Guilty Plea(s)	37.5
Yes, Trial Conviction(s)	12.5
No Pleas or Convictions	12.5
Case Still in Progress	37.5
	(N=8)

* Percents for Tables C7 and C8 are based on those 8 cases where Criminal Charges were filed (see Table C6).

Table C8. "Which of the following sanctions were imposed?"

	Percent*
Incarceration	25.0
Monetary Sanctions	37.5
Probation	25.0
A Warning or Reprimand	25.0
Other	12.5
Case Still in Progress	0.0
No Sanctions	0.0
	(N=8)

* Percents do not sum to 100.0 because more than one answer could be given.

Table C10. "Did any of the civil actions result in either a settlement for the company out of court or a trial judgement in favor of the company?"

	Percent*
Settlement Out of Court	45.5
Trial Judgment	18.2
No Favorable Outcome	9.1
Case Still in Progress	18.2
Don't Know	9.1
	(N=11)

* Percents for are based on those 11 cases which were referred for Civil Action (see Table C4).

Table C11. "What types of sanctions resulted?"

	Percent*,**
Injunction/Restraining Order	62.5
Asset Seizure/Forfeiture	37.5
Restitution	25.0
Fines or Penalties	50.0
Other	0.0
Case Still in Progress	12.5
No Sanctions	12.5
	(N=8)

* Percents are based on those 8 cases in which there was a "Settlement Out of Court" or a "Trial Judgment" in favor of the company (see Table C10).

** Percents do not sum to 100.0 because more than one answer could be given.

Table C12. "What administrative actions were taken as a result of this incident? In your opinion, which of these actions were especially effective?"*

	Taken Percent**	Effective Percent***
If Company Employee Involved		
Employee Terminated	87.2	73.5
Property Recovered/Restitution	51.3	70.0
	(N=39)	
If Outside Company Involved		
Contract Terminated/Suspended	38.5	66.7
Property Recovered/Restitution	28.2	72.7
	(N=39)	
Preventive Actions After Incident		
Tighter Management Controls	95.7	73.3
Tighter Security Measures	74.5	80.0
Improved Record Keeping	68.1	75.0
Changes in Employee Training	55.3	73.1
Improved Auditing Procedures	51.1	66.7
Changes in Contracting	25.5	91.7
	(N=47)	

* Table C12 includes only those administrative actions which were taken in more than 20 percent of the eligible cases. For "Company Employee" Actions, there were 39 eligible cases (i.e., cases in which administrative actions were taken and a company employee was involved); for "Outside Company" Actions, there were 39 eligible cases (i.e., cases in which administrative actions were taken and an outside company was involved); and for "Preventive" Actions, there were 47 eligible cases (i.e., all cases in which administrative actions were taken).

** Percents are based on the number of cases eligible to take each type of action (see preceding footnote).

*** Percents for each action are based on the number of cases in which that action was taken, ranging from 11 cases (for Outside Company "Property Recovered/ Restitution") to 45 cases (for Preventive "Tighter Management Controls").

D. Opinions About Trade Secrets Theft

Section D focuses on the opinions and attitudes of respondent security directors about the importance of the trade secrets theft problem; about the adequacy of current legislative and criminal justice (law enforcement and prosecution) strategies to deal with it; and about the potential effectiveness of these and a variety of company strategies for preventing theft incidents.

Most security directors (85%) considered the theft of trade secrets to be currently a "big" or "moderate problem" for U.S. companies in general (Table D1) and a majority considered it to be a problem in their type of industry, as well (Table D3). Although only about one fifth of the respondents viewed it as a current problem for their particular company (Table D4), almost two thirds felt it was "on the rise" (Table D2) and more than eight out of ten were "very" or "moderately concerned" about the victimization of their company in the future (Table D5). Over two thirds of the security directors said that this concern was shared by their company's top executives, as well (Table D6).

When asked about the most common types of trade secrets theft in their segment of the industry, three fourths of the respondents cited "current" or "former employees" as the most frequent initiators of thefts (Table D7a), most often from "technical or scientific" or "middle management" positions (Table D7b). These perceptions appear to be quite realistic, being consistent with the employment status of the actual offenders in the sample's most recent theft incidents (see Tables B17 and B19).

While fairly evenly divided about the adequacy of current state and federal criminal laws in helping to fight trade secrets theft (Tables D8 and D9), over 60 percent of the security directors said that law enforcement agencies were ineffective in investigating incidents (Table D12) and almost half viewed criminal prosecutors as ineffective, as well (Table D13). When respondents were asked to identify major criminal justice weaknesses in handling trade secrets theft cases, three were mentioned most often for both law enforcement and prosecution: "lack of expertise", "lack of resources", and "low priority given to these cases"(Table D14).

Despite their perceptions of criminal justice inadequacy, however, a majority of the respondents felt that American companies today were more inclined to refer trade secrets theft cases for criminal prosecution (Table D15) and over two thirds felt that companies were more inclined to take civil action (Table D16). These perceptions would seem to be based more on the absence of such referrals in the past than on a current inclination to pursue cases in the courts, since less than one fifth of the sample's "most recent incidents" were referred for criminal or civil action (see Table C4).

Finally, when asked to rate the potential effectiveness of a variety of company and criminal justice strategies for preventing trade secrets theft (Table D17), most of the alternatives were judged to be potentially "very effective" by about half of the respondents. The one strategy that appeared to be slighly more effective in the eyes of these security directors was "punishment of dishonest employees", which was rated as potentially effective by almost two thirds of the respondents. Given that most of these potentially effective company and criminal justice/legislative strategies were perceived to have current weaknesses by many of the security directors, improvements in these policie s and procedures could have a positive impact on the prevention and control of trade secrets theft in the future.

Section D Tables

Table D1. "Is theft of trade secrets currently a big problem, a moderate problem, or a small problem for U.S. companies in general?"

	Percent
Big	40.0
Moderate	44.7
Small	10.0
Don't Know	5.3
	(N=150)

Table D2. "Would you say this problem is on the rise, on the decline, or staying about the same?"

	Percent
On the Rise	63.3
On the Decline	.7
About the Same	28.7
Don't Know	7.3
	(N=150)

Table D3. "What about the theft of trade secrets in your type of industry --is it currently a big problem, a moderate problem, or a small problem?"

	Percent
Big	16.7
Moderate	40.0
Small	38.0
Don't Know	5.3
	(N=150)

Table D4. "What about the theft of trade secrets in your particular company -- is it currently a big problem, a moderate problem, or a small problem?"

	Percent
Big	2.0
Moderate	20.7
Small	69.3
DK	8.0
	(N=150)

Table D5. "How concerned are you about your company being a victim of trade secret theft in the future?"

	Percent
Very Concerned	44.7
Moderately Concerned	38.7
Not Very Concerned	13.3
Not At All Concerned	3.3
	(N=150)

Table D6. "How concerned are your top executives about your company being a victim of a trade secret theft in the future?"

	Percent
Very Concerned	28.0
Moderately Concerned	40.0
Not Very Concerned	21.3
Not At All Concerned	7.3
Don't Know	3.3
	(N=150)

Table D7a. "In your opinion, are trade secret thefts most often initiated by current employees, former employees, or outsiders?"

	Percent
Current Employees	48.0
Former Employees	26.7
Outsiders	18.7
Don't Know/No Answer	6.7
	(N=150)

Table D7b. "When employees or former employees are involved, [what positions] are they most likely to come from?"

	Percent
Blue Collar	3.3
Clerical	2.7
Technical/Scientific	55.3
Middle Management	30.0
Senior Management	2.7
Other	.7
Don't Know/No Answer	5.4
	(N=150)

Table D8. "In your opinion, how adequate are the current criminal laws in your state for assisting companies in the battle against trade secret theft?"

	Percent
Very Adequate	4.7
Adequate	39.3
Not Very Adequate	27.3
Not At All Adequate	6.7
Don't Know/No Answer	22.0
	(N=150)

Table D9. "In your opinion, how effective are the current federal criminal laws for assisting companies in the battle against trade secret theft?"

	Percent
Very Adequate	4.0
Adequate	32.7
Not Very Adequate	30.0
Not At All Adequate	6.7
Don't Know	26.7
	(N=150)

Table D12. "In your opinion, how effective are law enforcement agencies when it comes to investigating cases of trade secret theft?"

	Percent
Very Effective	4.7
Moderately Effective	19.3
Not Very Effective	44.0
Not At All Effective	16.7
Don't Know/No Answer	15.4
	(N=150)

Table D13. "In your opinion, how effective are criminal prosecutors when it comes to prosecuting cases of trade secret theft?"

	Percent
Very Effective	3.3
Moderately Effective	28.7
Not Very Effective	37.3
Not At All Effective	9.3
Don't Know/No Answer	21.3
	(N=150)

Table D14. "Below is a list of possible weaknesses in the state and local law enforcement and prosecution of trade secret cases. Please indicate which of these factors are major weaknesses in your opinion."

	Law Enforcement	Prosecution
	Percent	Percent
Lack of Expertise	78.0	61.3
Lack of Resources	71.3	57.3
Low Priority to These Cases	76.0	68.7
Lack Sympathy for Companies	46.0	46.0
Lack Cooperation w/ Security	24.0	20.7
Legal Restraints	37.3	35.3
Other Major Weakness	6.0	6.7
No Major Weaknesses	1.3	1.3
	(N=150)	(N=150)

Table D15. "Compared to five years ago, would you say that American companies today are more inclined or less inclined to refer a trade secret theft case for criminal prosecution?"

	Percent
More Inclined	59.3
About the Same	19.3
Less Inclined	11.3
Don't Know/No Answer	10.0
	(N=150)

Table D16. "Compared to five years ago, would you say that American companies today are more inclined or less inclined to take civil court action against trade secret theft?"

	Percent
More Inclined	70.7
About the Same	14.7
Less Inclined	8.7
Don't Know/No Answer	6.0
	(N=150)

Table D17. "In your opinion, how potentially effective are the following strategies for preventing the theft of trade secrets?"

	Percent*		
	Very	Somewhat	Not Very
Strict Auditing/Record Keeping	49.3	40.0	7.3
Strict Management/Supervision	52.7	39.3	6.0
Strict Security Procedures	58.0	36.7	3.3
Maintenance of Company Loyalty	48.0	34.7	15.3
Strict Employee Hiring/Screening	50.0	36.0	12.0
Employee Awareness of Secur Needs	54.7	37.3	6.0
Punishment of Dishonest Employees	66.0	24.7	6.7
Strict Criminal Justice Policies	50.0	32.0	12.7
Strict Legislation	46.7	35.3	12.7
Other Strategies	9.3	1.3	.7
	(N=150)	(N=150)	(N=150)

* Row percents do not sum to 100.0 because the "Don't Know" and "No Answer" responses are not included on the table.