1989

High-technology crime and public policy : a case study

Daniel E. Macallair
San Jose State University

Follow this and additional works at: https://scholarworks.sjsu.edu/etd_theses

Recommended Citation

Macallair, Daniel E., "High-technology crime and public policy : a case study" (1989). *Master's Theses*. 3090.

DOI: <https://doi.org/10.31979/etd.w8y2-eqvg>
https://scholarworks.sjsu.edu/etd_theses/3090

This Thesis is brought to you for free and open access by the Master's Theses and Graduate Research at SJSU ScholarWorks. It has been accepted for inclusion in Master's Theses by an authorized administrator of SJSU ScholarWorks. For more information, please contact scholarworks@sjsu.edu.

INFORMATION TO USERS

The most advanced technology has been used to photograph and reproduce this manuscript from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book. These are also available as one exposure on a standard 35mm slide or as a 17" x 23" black and white photographic print for an additional charge.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

U·M·I

University Microfilms International
A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
313/761-4700 800/521-0600

Order Number 1337824

High-technology crime and public policy: A case study

Macallair, Daniel E., M.P.A.

San Jose State University, 1989

U·M·I

300 N. Zeeb Rd.
Ann Arbor, MI 48106

HIGH-TECHNOLOGY CRIME AND PUBLIC POLICY: A CASE STUDY

A Thesis

Presented to

**The Faculty of the Department of Political Science
San Jose State University**

**In Partial Fulfillment
of the Requirements for the Degree
Master of Public Administration**

By

Daniel E. Macallair

May 1989

APPROVED FOR THE DEPARTMENT OF POLITICAL SCIENCE

A handwritten signature in cursive script, appearing to read "P. Haas", written over a horizontal line.

Dr. Peter Haas

A handwritten signature in cursive script, appearing to read "Dr. Kenneth P. Nuger", written over a horizontal line.

Dr. Kenneth Nuger

A handwritten signature in cursive script, appearing to read "Harry Allen", written over a horizontal line.

Dr. Harry Allen

APPROVED FOR THE UNIVERSITY

A handwritten signature in cursive script, appearing to read "Serena H. Stanford", written over a horizontal line.

Acknowledgements

I extend my deepest appreciation to Professors Peter Haas, Ken Nuger, and Harry Allen for their patient assistance and guidance throughout this project. I also thank my family, particularly my brother Mike and sister-in-law Barbara, for their support during the past five years. Without them, many of the opportunities I have had would not have been available.

ABSTRACT

HIGH-TECHNOLOGY CRIME AND PUBLIC POLICY: A CASE STUDY

By

Daniel E. Macallair

This research examines high-technology crime and the impact of law enforcement policy. Conclusions are derived from an evaluation of the District Attorney's Technology Theft Association (DATTA), which was an experimental program established by the California State Legislature. The program attempted to increase the level of criminal investigations and prosecutions in Santa Clara County, California by augmenting the investigative process. Conclusions were reached through a review of current criminal justice literature and through numerous interviews with leading practitioners and theoreticians in the field.

Though presently the data available is insufficient, preliminary evidence suggests that law enforcement intervention alone is not effective in reducing high-technology crime rates. However, there are indications that strengthening the investigative process raises the number of successful prosecutions. In addition there is evidence that suggests law enforcement intervention deters individual white collar convicted offenders from future crimes. Finally, the evidence also indicates that law enforcement policy is necessary and effective in maintaining the integrity of local police agencies.

Table of Contents

	<u>Page</u>
High-Technology Crime: The Growing Problem.....	1
Introduction.....	1
Problem Statement.....	2
Methodology	3
High-technology Crime	4
Computer Crime	5
Theft of Semiconductors.....	13
Theft of Trade Secrets	14
Causes of High-Technology Crime	15
High-Technology Crime Problems in Law Enforcement.....	17
Introduction.....	17
Investigating Computer Crime	17
Investigating Theft of High-Technology Material.....	21
Investigating Theft of Trade Secrets	24
Jurisdictional Fragmentation.....	26
Failure to Report.....	28
Lack of Deterrence.....	29
Summary.....	31
The Establishment of the District Attorney's Technology Theft Association (DATTA).....	32
Introduction.....	32
The Historical Foundation of DATTA.....	33
Pressure on Local Police.....	34

	<u>Page</u>
Mounting Public Awareness.....	35
1982 Race for District Attorney.....	36
The Creation of the DATTA Project.....	37
State Legislation Establishing DATTA.....	38
DATTA and Computer Crime.....	39
DATTA and the Theft of Semiconductors.....	40
DATTA and Trade Secret Theft.....	41
DATTA and Jurisdictional Fragmentation.....	42
Raising the Crime Reporting Rate.....	42
DATTA and Symbolic Reassurance.....	43
Summary.....	44
The District Attorney's Technology Theft Association:	
Its Implications for Future Public Policy.....	45
Introduction.....	45
DATTA's Impact on The Investigation of Computer Crime, Semiconductor Theft, and Trade Secret Theft.....	46
DATTA's Impact on Jurisdictional Fragmentation.....	51
DATTA's Effect on Reporting Rates.....	55
DATTA and The Deterrence Effect.....	58
DATTA and Symbolic Reassurance.....	62
Public Policy Considerations.....	63
Future Research Considerations.....	65
Conclusion.....	67
References.....	69

List of Tables

	<u>Page</u>
Table 1: Impact of DATTA Project on Criminal Processing.....	47
Table 2: Reasons for Not Reporting Instances of High-Technology Crime.....	57

List of Figures

	<u>Page</u>
Figure 1: Reasons for Not Reporting Instances of High-Technology Crime.....	56

High-Technology Crime: The Growing Problem

Introduction

In the past thirty years the American economy has undergone a profound and dramatic change. The decline of manufacturing-based industries has permanently altered the social and economic structure. The manufacturing industries were the backbone of the American economy for most of the past one hundred years. During this period the majority of the American work force were employed in blue collar production jobs. However, as technology progressed, the manufacturing sector was displaced from its dominate position and replaced by a new economic sector founded on high-technology. High-technology is any sector of the economy that is inextricably linked to advancements in science and technology. According to Larson and Rogers (1985):

A high-tech industry is characterized by: (1) highly skilled employees, many of whom are scientists and engineers; (2) a fast rate of growth; (3) a high ratio of R&D expenditures to sales; and (4) a worldwide market for its products. Not only is the technology very advanced, but it is also continuously changing, at a much faster rate of progress than other industries. Electronics is not the only high-tech industry today; genetic engineering is another, as are aerospace, pharmaceuticals, and instrumentation. Within electronics some sectors--like computers and semiconductors-- are based

on a technology that is advancing the most rapidly. So microelectronics is the highest of high-tech. (p. 29)

The emerging dominance of high-technology was first revealed in 1956, when demographers recorded for the first time in American history that white-collar information-processing jobs comprised the largest segment of the American work force. The significance of this change was noted by researcher John Naisbitt (1984):

Industrial America was giving way to a new society, where, for the first time in history, most of us worked with information rather than producing goods... . In 1950, only about 17% of us worked in information jobs. Now more than 65% of us work with information as programmers, teachers, clerks, secretaries, accountants, stock brokers, managers, insurance people, bureaucrats, lawyers, bankers, and technicians. (p.2)

This economic transition established the United States as a post-industrial society. In a post-industrial society the majority of the work force is engaged in the gathering, processing, and distribution of information (Rogers & Larson, 1985).

Problem Statement

As technology expands, the amount of high-technology crime is on the increase. Just as this new advanced technology can be applied to the benefit of society, it can also be used to its detriment. For instance, crimes involving information-based technology are now

confronting law enforcement officials with unfamiliar situations. Experts claim that, as the technology spreads, this unique crime problem will continue to worsen unless the law enforcement community is able to respond (D. Parker, personal interview, May 22, 1986).

The growing fear of high-technology crime is exerting pressure on policy makers to seek a solution. For example, some localities are diverting resources to bolster law enforcement efforts. These policies are founded on the belief that tougher police enforcement will reverse rising crime rates. In his study on the role of the public administrator, Simon (1957) stated the following: "It is his function to maximize the attainment of governmental objectives (assuming they have been agreed upon) by the efficient employment of the limited resources that are available to him ..." (p. 186). Therefore, on the subject of high-technology crime policy makers and public administrators will need to evaluate whether present law enforcement programs are effective in meeting their intended goals.

Methodology

This research has a four-fold purpose. First, it will illustrate and define the problem of high-technology crime and examine its causal elements. Second, it will review the current issues that are impeding the law enforcement community's ability to respond to the challenge. Third, this research will analyze the development of a

high-technology crime prevention program in Santa Clara County, California, and detail how this project addressed law enforcement deficiencies. Finally, the project will be evaluated based on a review of current criminal justice literature to determine its potential as a viable approach to combatting high-technology crime.

Because the subject of high-technology crime is still in its infancy, there is presently a dearth of reliable data. Information obtained for this research was gathered through an examination of both primary and secondary sources. This included numerous interviews with leading practitioners and researchers in the field. In addition, current published and non-published research and empirical data was also examined.

High-technology Crime

High-technology crime is defined by the California Legislature in Assembly Bill 1078 as:

... any violation ... arising out of the development or application of any technology requiring the most sophisticated scientific equipment and advanced engineering techniques such as microelectronics, data processing, genetic engineering, or telecommunication (State of California, 1984).

Under this legislation, the California Legislature concluded that high-technology crime was a serious problem that law enforcement was presently unprepared to deal with. Although other sectors of

the high-technology community are identified by this law, the electronics industry was its primary focus (D. Southard, personal interview, May 13, 1986). The electronics industry is responsible for the production of computers and semiconductors (Masuda, 1981). Because of the integral role this technology performs in the information age, certain individuals, who have the skills and knowledge to utilize this technology, will be in a position to wield an enormous amount of power, control, and influence (Southard).

Computer Crime

Presently, the most publicized form of high-technology crime is computer crime. Compared with more traditional crimes a computer allows a perpetrator to commit criminal acts with significantly greater speed, efficiency, and stealth (D. Parker, personal interview, May 22, 1986). Its effect is far reaching as the losses appear to be significant. For example, in 1984 the American Bar Association's Task Force on Computer Crime conducted a nationwide survey of 1,000 public and private organizations to determine the extent and degree of losses from computer-related crime. The responding organizations, reported computer crime losses that totalled between \$2 million and \$10 million (American Bar Association, 1984).

According to Donn Parker (1976), an international expert on computer crime at the SRI International: "Computer crime prominence results from high incidence, large losses, lack of

prevention capability, or great criminal leverage in terms of a large reward." Experts such as Parker of SRI and Jay Bloombecker of the National Center for Computer Crime Data, believe that computer crime is not only on the rise, but is also becoming more sophisticated (Markoff, July 24, 1987).

...It may not look like a growing problem, but underneath it has gradually and steadily increased in seriousness, he said. ... As modern society becomes more dependent on computer technology, it becomes more vulnerable, he added. It's a fragile world that we've created for ourselves, and it breaks easily.

Computer crime can be divided into the five categories of fraud and embezzlement, theft of services, mischief, theft of information, and attacks on computer resources (Schweitzer, 1986). Schweitzer argues that fraud and embezzlement are the most widespread because they are carried out by employees operating from inside the organizations. This claim is substantiated by arrests statistics gathered by the National Center on Computer Crime Data (Bloombecker, 1986). According to their research, the majority of computer criminals tend to be programmers, input clerks, and bank tellers. These individuals occupy positions that give them a complete understanding of the organization's operations.

A common form of computer fraud carried out by an insider involves the input of false data (Schjolberg, 1983). The process is

described in a recent study by the General Accounting Office (GAO) on Social Security fraud reported on by Spears (1985).

A few taps on a computer keyboard, a dishonest employee can create a fictitious person in the agency's computers ... a few more taps and benefit checks will be deposited directly into a bank account opened under a fictitious name. (p.13).

According to evidence gathered by the GAO researchers, between 1978 and 1982 there were 172 cases of fraud carried out with a computer in government entitlement programs. These cases averaged approximately \$45,000 in losses. The study points out that on the rare occasion when these crimes were discovered, it was usually by accident (Spears, 1985).

Embezzlement occurs when individuals steal money they have been entrusted to protect. Traditionally, this form of crime has been most prevalent in the banking industry. As banks have computerized their operations, new and more efficient ways of embezzlement have followed. For instance, one method of computer-assisted embezzlement that has emerged is the electronic transfer of small amounts of money from various customer checking accounts to other accounts secretly controlled by the perpetrator. These losses often escape detection because transfers take place at various intervals and the amounts are kept small and inappreciable. This type of theft is relatively simple and the risk of apprehension is low when compared to more common forms of white-collar crime,

because it can all be done without ever leaving the computer terminal and does not generate a paper trail (Schjolberg, 1983).

In addition to computer embezzlement and fraud, theft of computer services has become a serious problem for many organizations as the number of people competent in computer technology increases. Schjolberg (1983) offers the example of two directors of a technology company who used the institute's computer to manage three private businesses. These enterprises earned them over \$40,000 in profit. However, their unauthorized procurement cost the institute over \$200,000 by impairing the computer's ability to perform its primary function.

Embezzlement, fraud, and theft of services are usually carried out by people from within the organization who have authorized access to the computer. However, the most potentially destructive and notorious of all computer crimes comes under the category Sweitzer (1986) labels "mischief," which includes computer "hackers."

Computer "hackers" are individuals who use their home computers and telephone modems to infiltrate business and government computer systems. Evidence suggests that the number of computer "hackers" has swelled as the volume of home computers has increased (Maxwell, 1985). In addition, the activities of "hackers" often extend beyond mere mischief to include sabotage and theft (Markoff, July 24, 1987).

Computer "hackers" consider themselves an elite group with extraordinary skills at breaking into corporate and university computer systems,... "I can get into the telephone system computer," said one hacker. Lets say I don't like you. I can turn your telephone off or I can turn your telephone into a pay phone so it asks you to deposit 20 cents before making a call, or I can turn a pay phone into a free phone." (p.1)

Hackers have demonstrated remarkable ability to break secret codes that would prevent penetration of on-line computers. An on-line computer is a computer that an organization makes available to designated employees, customers, or clients to provide information and services. In a recent case, a group of West German hackers were able to break into a computer network operated by the National Aeronautics and Space Administration. Using a common hacker technique known as a "Trojan Horse," they were able to obtain information that was designated for a select group of scientists and researchers (Computer Sting, September 16, 1987).

A "Trojan Horse" is a term for a permanent program that enables amateur computer enthusiasts, or "hackers," to use a password to bypass all the security procedures of a system and gain access to all the data in a target computer. (p.17)

This program is developed once entry has been gained. At this point, the "hackers" simply design a program that instructs the computer

to allow them to enter. This does not preclude authorized user access, but it does allow the hackers to operate inside the computer without being detected.

An insidious type of Trojan Horse that has computer crime experts even more alarmed is the "virus." A computer virus is an altered computer program that is directed to continuously destroy data (Markoff, December, 1987).

Like their biological counterparts, computer viruses are tiny (no larger than several hundred bytes, each of which is equivalent to a single letter or number) and easily evade detection. Instead of invading living cells and taking command of its genetic machinery, they infiltrate an application program or an operating program--the computer's internal traffic cop.

Viruses can be created with such cunning that they're almost impossible to detect - initially. It may be months or years before they damage a system. (p. 1)

Many security experts believe that the potential threat is almost unlimited as long as computers are accessible through telephones. Many feel that the ability of a clever hacker to penetrate an on-line computer is almost unstoppable.

In addition to wider computer literacy, the spread of computer hacking has been facilitated by the proliferation of computerized bulletin boards (BBS's). A computer bulletin board is a means for

computer users to share and disseminate information. Most bulletin boards are operated out of a private residence. With a home computer, modem, and proper password, an individual can access the bulletin board and obtain whatever information it holds. According to computer crime consultant John Maxfield (1985):

It is very easy to become addicted to BBS's and the strange electronic underground that is associated with them. While a BBS is not inherently an evil thing, it does tend to contribute significantly to electronic crime. (p.2)

Information sharing among electronic bulletin board users has led to an increase in the number of people with access to illegal information. This information can include (Maxwell, 1985):

Lists of phone numbers of famous people, government installations, computer systems, and telephone operator call routing codes.

Lists of credit card numbers (i.e. VISA and MASTERCARD) to be used to order merchandise over the phone for resale or trade.

[Information on how] to invade the privacy of anyone through access to their computerized credit and financial records. (p.6)

The danger of bulletin board misuse was dramatized in a recent case in New Jersey that resulted in the arrest of seven

juveniles, who were using an electronic bulletin board to disseminate the secret codes to the computers of American Telephone and Telegraph Company. This information included highly sensitive and classified information on international communication satellites systems. With this information they could have redirected the satellite's orbital position, thus interrupting intercontinental transmissions. In addition, they were also found to be exchanging instructions on how to alter AT&T customer billing codes, and information on illegally obtained credit card numbers (German Hackers, 1985).

Computer-related high-technology crime also appears to be challenging the applicability of many traditional laws and practices. For instance, computer technology prevents protecting valuable information through mere physical security.

Computers now make it possible to electronically eavesdrop on private transmissions with remarkable ease. Through electronic eavesdropping, valuable information can be obtained that may harm the owner trying to protect it. For instance, with a computer, the personnel of one business can intercept and monitor the communications of another. Under current laws this may not be a crime because the owner is not being deprived of the information and no tangible property is being taken. Although many legislatures have moved to address this gap by designing new statutes, enforcement remains a major question (Schrage, 1985).

The last area of computer crime involves direct physical assaults on the computer, which would be considered sabotage and vandalism. Although these crimes are more conventional in nature and do not require any specialized knowledge, they often result in the greatest monetary loss. A company dependent on a computer to conduct the bulk of its business can be devastated by the loss of not only the information, but also the means to recuperate quickly (Parker, 1976).

Theft of Semiconductors

Another element of high-technology crime is the theft of advanced electronic materials, such as semiconductors. In Santa Clara County, California, losses from thefts of semiconductors, which are also known as "chips," have been estimated at \$20 million a year (D. Southard, personal interview, May 13, 1986).

Semiconductors are the most vital component of the electronics industry, because they embody the mechanism that allows for rapid information processing, transference, and storage. Unfortunately, because of their minute size and the high volume of production, they are easily stolen. In some cases thefts are so serious that entire company inventories are depleted (Rogers & Larson, 1985). However, the average theft tends to involve employees slipping individual chips into their pockets and walking out the company gate. Then the chips are sold to dealers, who then

sell them to other buyers (D. Southard, personal interview, May 13, 1986).

The theft of semiconductors in the electronics industry has proven to be a highly unique crime, because materials are so small and production is so rapid that companies cannot produce immediate evidence that an illegal act took place. As a result, investigations are rare because police will not pursue the case without tangible evidence from the company (J. Hacker, personal interview, September 11, 1986).

Theft of Trade Secrets

As the electronics industry has rapidly advanced, it has become intensely competitive. This competition places a premium on innovation. In this continuously changing market, if a company is to thrive it must be adaptive and innovative (Larson & Rogers, 1985).

In this competitive market, a computer or semiconductor design can determine a company's viability. As a result, individuals and companies often try to gain an immediate market share by stealing the trade secrets of their competitors, such as the plans to a new computer or semiconductor. The continual theft of company secrets can have a long-term deleterious impact on innovation, since it discourages investment in research and development (D. Southard, personal interview, May 13, 1986). If a company cannot gain from

its innovative designs, its ability to recoup its investments in research and development is forfeited, and its survival is imperiled.

Causes of High-Technology Crime

According to criminologists, motivation and opportunity are the basis of criminal activity. For instance, it is estimated that 10% of the population will never commit a crime while 10% frequently will. The remaining 80% harbor the potential to engage in unlawful acts if favorable circumstances exist (Swartz, 1982). Therefore, in the case of high-technology crime, Swartz estimates that 90% of all computer operators are potential security risks.

In examining computer crime, Swartz (1982) argues that the motivation for these acts emanates from the perception of the computer as an easy victim. According to Swartz, "these crimes are easily covered, no audit trail is left behind and assuming the new felon is an insider and greedy he can carry on his malfeasance for a long time." Therefore, according to this precept, high-technology crimes, like other forms of crimes, will thrive if they are perceived to carry minimal risks.

In a 1979 study of computer fraud, Krause and MacGahan (1979) found that motives for computer criminals do not differ from those who engage in other forms of illegal activity. Krause and MacGahan identified six primary characteristics that compel people to engage in high-technology crime. These are (Krause & MacGahan):

1. Avarice, which is the desire of individuals to augment their income to achieve a higher standard of living;
2. Desire for material possessions such as a compulsive desire for an expensive automobile;
3. Financial problems which arise from over-purchasing or living beyond one's means;
4. Ego gratification which results from conquering a complex technological device;
5. Robin Hood Syndrome which results from the belief that high-technology crime inflicts harm only on large impersonal organizations and does not victimize individuals. Many perpetrators rationalize this as getting even for the harm these organizations have wrought on society; and
6. Revenge which occurs when individuals feel that they have been treated unfairly and thus feel a need to retaliate. (p. 46)

These are the most commonly-cited reasons that could dispose a person towards criminal activity. Parker (1983) and other experts suggest that, as long as high-technology crime continues to involve little risk, many individuals will be willing to seize the opportunity. Therefore, if such behavior is to be deterred, the risk of apprehension and punishment must increase significantly. However, if law enforcement practices do not adapt, than this is unlikely to occur.

High-Technology Crime Problems in Law Enforcement

Introduction

Law enforcement officials and private experts believe that initiating a viable response to high-technology crime will require major advancements in the training and preparation of police investigators. Experts contend that improving the investigative capacity of the police will result in more arrests and prosecutions and deter future criminal activity (Bequai, 1978). This chapter outlines the primary issues considered crucial to improving the investigation process in the area of high-technology crime.

Investigating Computer Crime

Presently, the preponderance of literature on high-technology crime is devoted to computer crime. This is due to the computer's growing ascendancy as the central element of our economy. For example, Cira (1983) writes that the "computer is becoming the vault for the business community and government. But, there is growing evidence to indicate that the vault is seriously vulnerable to criminal exploitation" (p. 37). According to Swartz (1982), the average monetary loss from a computer crime is approximately \$400,000. This figure appears staggering when compared to the average \$10,000 and \$20,000 monetary losses that result from a traditional bank robbery or bank embezzlement.

Cira (1983), believes that the development of an effective policy against computer crime should be founded on two goals

1. how to reduce the incidence of any crime in which a knowledge of computer technology is needed to understand the intentional acts that result in losses; and
2. how to successfully investigate the crime and develop evidence for the prosecution of perpetrators. (p.37)

Cira feels that the major obstacle to an effective campaign against computer crime is the lack of specially-trained investigative personnel. Proper knowledge is essential since the process of extracting information from a computer is extremely complicated and beyond the capacity of the untrained layman. Unfortunately, there are few law enforcement investigators at the local, state, or federal level who have the competence or the experience to organize and conduct a proper computer-crime investigation (Swartz, 1982).

This bleak assessment is corroborated by studies by Donn Parker (1976) at SRI International. Parker believes that only a small percentage of computer crimes are ever detected, and an even smaller number are successfully prosecuted. This is supported by estimates indicating that "only one of the estimated 200,000 computer crimes committed this year is likely to be prosecuted" (Swartz, 1983, p. 5).

The current situation will only worsen as more assets become computerized, causing investigations to become even more complex. Parker (personal interview, May 23, 1986) states that, the more difficult a crime is to investigate the less likely it is to be successfully prosecuted. Many in law enforcement believe that these crimes are going unchallenged because of an inherent tendency among investigators to avoid the unfamiliar (Bequai, 1987).

According to Moulton (1983), computer crime confronts investigators with a new set of circumstances.

Computerized evidence is not the same as other forms of physical evidence. The particular difficulty with computer related evidence is that it is frequently invisible in its original form and can be easily modified or destroyed. (p. 49)

Unless evidence is gathered there can be no prosecution and if there is no prosecution, there is no enforcement of the laws. If the threat of discovery and apprehension is perceived to be low, then the frequency of the illegal act is likely to increase. Bequai (1978) believes this is the situation with computer crime.

Local law enforcement lags behind in the area of computer crime, felons have, for many years wreaked havoc in this area. What has spared us is our ignorance of what goes on, rather than our ability to deal with it effectively. (p. 23)

Electronic impulses are the means in which the computer receives and stores information. When these electronic impulses become the only means of generating crucial information to obtain evidence, the investigation inevitably becomes highly complex. It is in these cases where current deficiencies in computer crime investigations are manifested. As a result, in cases where evidence must be taken from computer-stored information, Parker (personal interview, May 22, 1986) believes that not only is it important for investigators to have an elementary understanding of the computer technology, but they must also be able and willing to obtain the assistance of an expert. Parker warns that, in cases of computer crime, the investigator is confronting a perpetrator who has a thorough understanding of the particular computer system, and who is adroit at concealing his or her actions. If an investigation is attempted by someone without a complete knowledge of the computer system, the risk of disregarding or destroying important evidence is greatly increased.

Unfortunately, most local law enforcement agencies are currently incapable of conducting adequate investigations and they are poorly prepared to procure qualified experts. For example, Parker (personal interview, May 22, 1986) cites a case of a small company who maintained all their records on a fixed computer disk. When an incident of malfeasance involving the computer was suspected, the proprietor reported it to the local police. Lacking any knowledge and experience with computers, the two investigators

assigned to the case recruited a self-described computer hacker from a local college who claimed to understand the particular system. Unfortunately, due to the investigator's lack of expertise and the ineptitude revealed by their consultant, the case resulted in the erasing of all the information contained on the disk. This led to the eradication of all possible evidence and to the eventual bankruptcy of the company.

According to Sergeant William Carver (personal interview, May 23, 1986) of the City of Santa Clara's Police Department, who has conducted numerous investigations of computer-related crimes, obtaining evidence from computer records is one of the most difficult tasks confronting investigators. He believes that, if investigators are to have any chance in protecting property and enforcing the law, new preparation and training methods must be developed

Investigating Theft of High-Technology Material

High-technology crime also includes the theft of specialized materials. Among the most troublesome problems plaguing the electronics industry is the theft of semiconductor chips (personal interview, J. Hacker, September 11, 1986). Since these chips are perhaps the most vital component of modern information technology, their protection is considered essential by the companies that produce them.

Due to their diminutive size and the high volume of production, the theft of semiconductor chips is extremely difficult to detect. For instance, Marv Zitke (personal interview, May 18, 1986) Chief Security Officer at Intel, one of the nation's largest producers of semiconductors, says that it is easy for an employee to smuggle out large numbers and sell them on the street in the "grey market."

This grey market has facilitated a rise in chip thefts. Rogers and Larsen (1984) give the following description:

... an active "grey market," a system of middlemen both legal and illegal, who distribute chips from the semiconductor houses to small quantity buyers such as certain computer and other firms (large customers like Intel, National, and Fairchild buy directly from the semiconductor manufacturers).

Sometimes the small buyers are in a hurry to buy chips, or are anxious to get a cut-rate price. These are conditions that foster the theft of semiconductors; as they pass through the grey market, the chips may lose their source of origin, thanks to cooperative middlemen who conveniently overlook it ...

(p. 186)

Another reason chips fall into the grey market is the lack of adequate internal security within the electronics industry. For example, it is not uncommon for faulty chips to be discarded in company dumpsters. These chips are then salvaged by unscrupulous suppliers and sold. In the past, these chips have been discovered in

medical equipment and national security computer systems (D. Southard, personal interview, May 13, 1986).

Because chips are produced in such high volume it is not possible to maintain precise records of the number manufactured. As a result, in many cases companies do not know when a theft has occurred. Even when theft is suspected, they are unable to establish proof since records are not available of every chip produced. Carver (personal interview, 1986) states that thefts of semiconductor chips are usually only discovered when they start showing up in the grey market. Therefore, the investigation of stolen semiconductors requires sophisticated undercover investigations. The most common method employed is the "sting" (Santa Clara County Sting, 1984). In a sting operation an undercover investigator goes out into the community posing as a potential buyer to establish contact with a person suspected of selling stolen chips. Once contact is established, the investigator attempts to purchase a quantity of chips from the dealer. If the person is able to produce the chips, an arrest is made (P. Moore, personal interview, June 12, 1986).

Another method frequently employed in these cases is the reverse sting. In a reverse sting a person is targeted who is believed to be receiving stolen chips. In this instance an undercover investigator contacts the individual and offers to sell alleged stolen chips. If the person agrees to the purchase, he is arrested for receiving stolen property (P. Moore, personal interview, June 12, 1986).

One problem that has emerged in the area of stolen chips is that law enforcement agencies are often not prepared or willing to conduct investigations on these matters. The attitude prevails among many in law enforcement that the responsibility to determine theft rests with the company. This has led to a reluctance among police agencies to involve their personnel in these matters (M. Zitke, personal interview, May 5, 1986).

Investigating Theft of Trade Secrets

Another perplexing area of high-technology crime is the investigation of trade-secret theft. A trade secret is defined as:

Any formula pattern, device, or compilation of information which is used in one's business, and which gives him the opportunity to obtain an advantage over competitors who do not know or use it. The only requirements are actual secrecy and some degree of novelty. A trade secret is given effect when it is agreed to by contract, enforced by a confidential relationship, or when the knowledge is gained by improper means. (Stein, 1985, p. 1039)

As in computer crime, success in trade-secret theft investigation hinges on the investigator's familiarity with the technology being investigated. Unfortunately, most police agency staffs do not possess this type of knowledge and many

investigations have been stymied as a result. For instance, in a recent case in Santa Clara County, California:

A technician at a major laser manufacturer called the president of a rival company and offered to sell him plans for his employer's product. The company president called the police, but when an undercover agent was sent to negotiate the deal, the technician backed off because he suspected the officer did not know anything about lasers (Computer Crime Digest, 1983, p.3).

Trade secret information can often run into the millions of dollars. The recent case of Peter K. Gopal presents a vivid example of the many difficulties inherent in trade secret theft investigation.

Peter Gopal, through various inside contacts in a number of semiconductor industries in Silicon Valley, was able to obtain "hundreds of computer tapes, masks and other design materials from Intel, National Semiconductor, Zilog and other companies." Because much of this information contained "state of the art" innovations that had yet to be marketed, the estimated dollar loss was into the millions of dollars (Southard, 1982).

In addition, the investigation found evidence to indicate that Gopal was involved in an international transaction that included the Soviet Union and Poland.

A business associate ... told authorities that Gopal bragged of having purchased certain testing equipment and selling it to

A business associate ... told authorities that Gopal bragged of having purchased certain testing equipment and selling it to Poland via one of his Swiss intermediaries. (p. 146)

Gopal was indicted and charged with possession of stolen trade secrets worth millions of dollars. Although he was eventually convicted after a protracted six month trial, the case highlights the problems that currently confront investigators and prosecutors. For example (Southard, 1982):

Neither the prosecution nor defense was willing to risk a jury trial because the issues were so complicated. At one point a judge threw out most of the physical evidence because the police officers serving search warrants were so ignorant as to what they were looking for, they had to take technical people along with them just to identify what was stolen and what was not. (p 148)

In this case, the prosecution was assisted when the State Court of Appeals overruled the lower court and allowed the evidence to be admitted (D. Southard, personal interview, May 13, 1986).

Jurisdictional Fragmentation

The Gopal case was also significant because it demonstrated the problem of conducting investigations that involve multiple jurisdictions. Bequai (1976) notes:

... there are currently over 17,000 local police forces ... law enforcement is made up of small, separate groups, acting independently of the other and many times in ignorance of what an adjoining jurisdiction is doing. (p. 46)

It is common for high-technology crimes to transcend the jurisdictional boundaries of local police forces. This complicates the investigative process because success depends on the cooperation and competence of a variety of independent agencies.

Southard (1982) feels that many high-technology crime cases are beyond the capability of a single local law enforcement agency. For instance, in citing the Gopal case, a complete and comprehensive investigation was precluded because of the number of agencies that would have been involved. As Southard (1982) later stated:

If we were really going to go all the way to prove out the chain of evidence, tracing the parts from Germany back to their theft source in California it would require the exhaustion of the entire witness budget of my county for the whole year.

(p. 147)

This is an inherent problem with the American criminal justice system. The implication is that any law enforcement policy focused on high-technology crime must be designed to improve cooperation and coordination between multiple and diverse agencies.

Failure to Report

Jacobs (1984) writes that in most criminal cases police determine what occurred through the testimony of victims. The evidence shows that "police success depends more on swift citizen response and accurate recall than on fancy police work or equipment" (p.46). Unfortunately, a chronic problem that has impeded the development of police responses to high-technology crime is the reluctance of business managers and executives to notify local authorities when they have been victimized.

U.S. Attorney Robert Fiske (1978) attributes this to an inherent fear among executives of the possible ramifications if creditors, stockholders, and clients became aware that the company's financial or material assets are vulnerable. By acknowledging that their security can be breached, managers fear that their company's competitive position and their personal prestige will be compromised.

In addition, Parker writes that companies often risk more from consequential loss by reporting computer crimes than they do from the direct cost of the crime. According to Parker (1986), "The consequential cost is the total monetary, human, and resource losses that occur, sometimes for years, after the incident" (p. 147).

Consequential losses are incurred when a company attempts to provide police and prosecutors with staff or material assistance. In addition, consequential losses often escalate when the crime is

made public resulting in a loss of confidence in the company's management practices (Parker, 1986).

Parker (personal interview, May 22, 1986) states that due to possible consequential losses, he is compelled to advise his business clients that reporting high-technology crimes to authorities may have serious adverse ramifications. However, Parker states that he balances his advice with a reminder to companies that they have a moral obligation to society and to their customers to make these incidents known. He believes that each company must decide individually on how it will respond to this dilemma.

Parker (personal interview, May 22, 1986) feels that a successful public policy response to high-technology crime must strive to create an atmosphere of trust and confidence between the criminal justice system and the business sector. Bequai (1978) believes that one reason businesses are reluctant to cooperate in this area is that they are aware of law enforcement's inexperience in dealing with these crimes. Therefore, the law enforcement community must develop a more competent profile if the concerns of the private sector are to be allayed.

Lack of Deterrence

A number of criminal justice practitioners believe that the ambivalence exhibited by industry towards crime reporting inhibits any potential deterrent effect. Fiske (1978) states that deterrence

is predicated on the belief that people are less likely to engage in unlawful activity if they perceive that the risks of being caught are great.

The most effective deterrent to crime in business is the realization that when that crime comes to the attention of people in business it is going to be reported and prosecuted so that other people in business when they learn about that, appreciate the fact that if they commit crimes, they are going to get caught and be punished. (p.12)

Therefore, any business taking a position not to report these crimes reduces the risk of catching offenders and thus eliminates any deterrent impact. It is widely felt among police and prosecutors that the absence of a deterrent effect will result in an increase in the frequency of crime (D. Southard, personal interview, May 13, 1986).

According to Conklin (1981), white-collar crime may be more susceptible to deterrence than other forms of crime. For deterrence to exist a criminal act must be a rational choice where the perpetrator has carefully weighed the potential gains against the possible losses. Because white-collar crime usually involves a high degree of planning, the likelihood that perpetrators will consider the possible consequences is higher.

Conklin (1981) believes that detection is the most crucial element in deterring white-collar offenders. For instance:

Detection means social embarrassment and the loss of influence in the business world. White-collar offenders, including corporate executives, computer thieves, and department store employees, seem to be more sensitive to the loss of face and social status than to the possibility of prosecution and imprisonment. (p. 399)

To support this contention, Conklin attributes a low rate of bank embezzlements to the banking industry's willingness to report these crimes to authorities when they occur. He claims that this has resulted in a high rate of prosecutions, which has led to lower incidence of this particular crime. This suggests that a deterrent effect does exist in the area of white-collar crime, but its existence is contingent on a diligent industry-wide reporting policy, combined with prompt police action.

Summary

The current belief among those in the law enforcement establishment and a number of computer experts is that high-technology crime can be reduced if these issues are adequately addressed. Lack of respect for police and their ability to meet the challenge will lead to an unimpeded growth in these crimes. This hypothesis assumes that the problem can be solved by mobilizing and improving the resources of the law enforcement community and by building a cooperative link with the private security sector.

The Establishment of the District Attorney's Technology Theft Association

Introduction

The world's largest concentration of high-technology industry is located in Santa Clara County, California. As this industry has grown, it has assumed a vital and influential role in the local economy. However, with their economic expansion, high-technology companies in general, and the electronics industry in particular, have become the victims of a growing number of high-technology crimes. According to a report issued by the State of California's Office of Criminal Justice Planning (OCJP) (1987):

In the mid 1970's, intense competition and heavy demand for semiconductor chips contributed to the growing problem of chip theft and other high-technology crimes. The Santa Clara County District Attorney's Office reported a yearly progression of reported chip thefts from 1978 to 1982. By the late 1970's it became clear that local law enforcement was ill-equipped to investigate and prosecute the kinds of crimes related to these industries. (p. 1)

In response, the first comprehensive high-technology crime prevention program in California was instituted in 1984. The project was designed as a three-year pilot program targeting high-technology crime in Santa Clara County. Its main purpose was to bolster the resources of local law enforcement agencies through

better training, interagency coordination, and private sector assistance. This program was called the District Attorney's Technology Theft Association (DATTA) (Robert Elliot, personal interview, September 5, 1987).

The Historical Foundation of DATTA

The foundation of DATTA can be traced to a major trade secret theft in 1974 at an IBM plant in San Jose. According to Deputy Santa Clara County District Attorney Douglas Southard (personal interview, April 13, 1986), the publicity generated by this event aroused concern among local industry security managers. As a result, in the late seventies a group of senior security managers from the major electronics companies in Silicon Valley began gathering on an informal basis to discuss their security needs. Soon, a number of the participants in 1978 formally organized the group into an association called ISMG, the Industrial Security Managers Group (D. Southard, personal interview, May 13, 1986).

Former ISMG president Wayne Dexter (personal interview, April 21, 1986) states that the group provided a means for senior security managers to discuss their common concerns. Since the companies perceived a growing threat to their security, the need for a comprehensive response was a major topic.

According to Hewlett-Packard Security Director, James Hacker (personal interview, September 11, 1986), it was agreed among the group that a comprehensive solution required the participation of

the law enforcement community. Therefore, the ISMG initiated the first effort in Santa Clara County to develop a cooperative link between private industry security and public law enforcement. To formalize this commitment, the following mission statement was adopted for its charter:

A major responsibility of this industrial group will be to concentrate on improving the relationship between the public sector and the private industry; providing a forum for the identification of common problems and working together to develop programs to correct them. (ISMG, 1978, p.1)

Pressure on Local Police

In 1978, ISMG representatives began lobbying local police for the purpose of raising the level of concern about high-technology crime. The most vocal of these representatives was John O'Laughlin, security manager at Intel and the first president of the ISMG (P. Moore, personal interview, July 12, 1986). Up to this time the response by local police to high-technology crime was woefully inadequate. According to Hacker (personal interview, September 11, 1986) this was attributable to an "avoidance syndrome" that pervaded the law enforcement community. Because of the complexity inherent in high-technology crime, police investigators were reluctant to attempt investigations. On the rare occasion when police were summoned to crime scenes, they would simply take a

report and depart without ever contacting the company again (James Hacker, personal interview, September 11, 1986)

As a result, Mr. O'Laughlin began holding special training sessions for members of the Santa Clara County Sheriff's Department for the purpose of familiarizing them with the intricacies of high-technology crime investigation. This marked the first attempt ever in Santa Clara County that police investigators were specifically trained in high-technology crime investigation (P. Moore, personal interview, July 12, 1986).

Mounting Public Awareness

At the time the ISMG was being formed in 1978, a number of well publicized high-technology crimes occurred that brought the issue farther into the public spotlight. In September 1981, Peter K. Gopal was apprehended with hundreds of computer tapes, circuit designs, and masks worth millions of dollars from such companies as Intel, National Semi-conductor, and Zilog. These materials were some of the most advanced engineering secrets in the industry, with many still in the developmental stage. Whoever could obtain this information could gain a decided advantage in the highly competitive semiconductor market. In addition, investigations by the Santa Clara County Sheriff's Department and the United States Commerce Department indicated that Gopal may have been selling these secrets to Soviet Bloc countries. Because of these serious issues this case

vividly illustrated the dangers of trade secret theft (Southard, 1982).

Another event with a different public policy implication was the case of Larry Lowery. Lowery masterminded the theft of \$3.4 million worth of integrated circuits from Monolithic Memories in Sunnyvale, California. This constituted almost 20% of the company's inventory. When the incident was discovered, the company immediately reported it. Unfortunately, the City of Sunnyvale did not have personnel with the expertise to conduct a proper investigation (D. Southard, personal interview, May 5, 1982). As a result, personnel from the County Sheriff's office, who had received previous training from ISMG President John O'Laughlin, were called in to provide assistance. The case was eventually solved by the Sheriff's Department investigators who posed as grey market chip buyers in a "reverse sting" (D. Southard personal interview, May 13, 1986).

The Lowery case was important for two reasons. It revealed significant deficiencies within some local law enforcement agencies, and it obviated the urgency for increased police awareness of high-technology crime issues (D. Southard, personal interview, May 13, 1986).

1982 Race for District Attorney

These revelations, combined with continuing pressure from industry, prompted local elected officials to react. As the

challenger in the 1982 campaign for Santa Clara County District Attorney, Julius Finkelstein made the topic of high-technology crime a major issue in his campaign to oust incumbent Leo Himmelsbach (Kaye, 1982, p.1B).

Finkelstein mounted an effective challenge by advocating the creation of a special task force to specifically fight high-technology crime. This position enabled him to win endorsements and donations from a large number of high-technology companies. He eventually lost the race by only 4,100 votes (Kaye, 1983, p.1B).

In response to Finkelstein's challenge, Himmelsbach promised that one of his initial policy changes would be the formation of specialized units within the District Attorney's Office to prosecute specific types of crimes. These units would acquire the requisite knowledge and skills to effectively prosecute cases in their particular areas (Kaye, 1982, p. 1B).

The Creation of the DATTA Project

The 1982 campaign for Santa Clara County District Attorney established high-technology crime as an important political issue in the county. Soon after the election, the district attorney's office began developing the county's first high-technology crime task force. In Computer Crime Digest (1983) Himmelsbach expressed the following reason for its founding:

What happened in the past is that we haven't been equipped to handle the problem ... The average detective is trained in street

crime, robberies, forgeries and so forth. They didn't know the lingo of the industry. Since they lacked the background they lacked confidence and commitment. (p. 3)

The mission of this new task force was to provide training and assistance to law enforcement investigators in high-technology crime. It was called the District Attorney's Technology Theft Association (DATTA).

State Legislation Establishing DATTA

In 1984, Himmelsbach, with the support of local industry, sought state assistance to expand the project. Under the sponsorship of State Assemblyman Dominic Cortese, the legislature passed Assembly Bill 1078, which provided a State grant of \$238,216 to establish the DATTA project as a three-year pilot program (R. Elliot, personal interview, September 21, 1987). According to the legislation the goal of the program was to:

Reduce high-technology theft in California ... arising out of the development or application of any technology requiring the most sophisticated scientific equipment, and advanced engineering techniques such as microelectronics, data processing, genetic engineering, or telecommunications. (State of California, 1984, p.4)

Policy makers sought to limit high-technology crime by improving the knowledge and resources of law enforcement

personnel. Due to the electronics industry's dominance of the Santa Clara County economy, DATTA's primary focus was computer crimes, semiconductor thefts, and trade secret thefts.

DATTA and Computer Crime

To address the problem of computer crime, DATTA conducted training sessions on computer technology and the various criminal acts associated with it. The purpose was to provide investigators with a general knowledge of computer technology. As experts note, law enforcement's understanding of computers lags far behind that of computer criminals (Bequai, 1986). Narrowing this gap requires investigators to have a basic understanding of computer systems.

Along with training in computer technology, DATTA's mission was to bolster the ability of investigators to use experts. As Parker (personal interview, May 22, 1986) points out, the effective investigation of computer crime necessitates the assistance of experts. However, few police agencies understand how to properly obtain and utilize private professionals. Even in the instance when police investigators have training in computers, experts are still essential due to the broad diversity of computer systems. According to Volgyes (1980):

Though it is clear that the investigation of computer-related crimes requires familiarity with electronic data processing, auditing, and accounting, investigators do not need to be computer experts. They do need to understand the system

enough to use the knowledge of computer specialists in tracking possible crime. Police investigators must realize the necessity of cooperating with computer experts to ensure that they will obtain the type of evidence necessary to apprehend computer criminals. (p.395)

No single investigator, no matter how thorough the training, can have more than a general knowledge of most systems. Therefore, DATTA's objective was to train police investigators to identify the source of the needed evidence and then to locate the proper expert to retrieve it (R. Elliot, personal interview, September 21, 1987).

DATTA and the Theft of Semiconductors

Curbing the the theft and distribution of semiconductor chips in Santa Clara County required an understanding of the magnitude of the problem and an increased willingness among police agencies to take a more active role. Despite the serious economic losses from chip theft in Santa Clara County, law enforcement agencies had never mounted a campaign against it. Therefore, DATTA sought to convince law enforcement agencies that they must assume the initiative on this matter rather than just wait for a victimized company to first report a loss.

In addition to seizing the initiative, investigating the theft of semiconductor chips requires police personnel in Santa Clara County to understand how to infiltrate the grey market. The key to success in breaking illegal operations is knowing what to look for. For

instance: "One of the best ways is to monitor the grey market and when an unusually low-priced sale occurs, the police investigate it" (Larson & Rogers, 1984, p. 187). By teaching techniques of undercover operation that specifically relate to the theft of semiconductor chips, DATTA planners hoped to significantly increase the level of prosecutions in this area (R. Elliot, personal interview, September 21, 1987).

DATTA and Trade Secret Theft

On the issue of trade secret theft, DATTA's training focused on the investigation process and the application of new trade secret laws. California is one of the few states to have enacted a law designed specifically to protect trade secrets. Under California Penal Code section 499c information is identified as a tangible asset. According to researchers Nycum, Snow, Bartlett, and Parker (1986), "The California law expressly proscribes stealing, taking, carrying away, or using, fraudulent appropriation, and unlawful or lawful access followed by a wrongful copying of the trade secret" (p. 6).

This law is particularly applicable to the electronics industry since it protects trade secrets and allows for an attachment of a monetary value to information (S. Nycum, personal interview, November 4, 1986). Due to this provision, an investigator can now build a criminal case based on the estimated value of the information. Under previous criminal statutes this was not possible.

Therefore, investigations of trade secret theft present investigators with a new set of circumstances and challenges that requires a knowledge of the applicability of these new laws (D. Parker, personal interview, May 22, 1986).

DATTA and Jurisdictional Fragmentation

In Santa Clara County there are 18 different local law enforcement jurisdictions, not including numerous state and Federal authorities. As in most areas of the United States, each jurisdiction is an autonomous unit with individual priorities. Therefore no single government unit controls all the portions of law enforcement policy (Yates, 1977). Jacobs (1984) explains, that due to this situation, "No uniform policy targeting a particular kind of crime can be implemented over a whole metropolitan area; each department has its own policies and methods ..." (p. 18).

As a result, DATTA's objective was to convince the multiple agencies to participate voluntarily in the project. Once participation was secured, DATTA's challenge was to maintain each agency's commitment. This necessitated creating a favorable environment capable of breaking down artificial barriers and engendering cooperative efforts.

Raising the Crime Reporting Rate

The reluctance of businesses to report crime to the police is regarded by criminal justice experts as a major impediment to

effective law enforcement. However, presently companies have little incentive to report crimes to the police since reporting results in additional financial costs while yielding negligible tangible returns (Parker, 1986).

According to Elliot (personal interview, 1987), if DATTA were successful in creating a positive and cooperative relationship with the private sector, the rate of reporting would rise. This is based on the belief that companies were unwilling to report crimes because of the lack of cooperation previously exhibited by law enforcement. According to the conclusions of the California Office of Criminal Justice Planning (Annual Report to the Legislature, 1987):

The lack of coordination between industry and law, enforcement contributes to non-reporting of high-technology crime. Non-reporting of crime is a major stumbling block to the development of a crime prevention strategy. (p. 15)

It was hypothesized that DATTA would reverse this problem through improved training and better communication (R. Elliot, personal interview, September 5, 1987).

DATTA and Symbolic Reassurance

According to Decker, Smith, and Uhlman (1979), followed by crime suppression, the primary functions of police are, first, symbolic reassurance. The symbolic reassurance role is predicated on the importance of maintaining a competent image to insure

agency legitimacy within the community. Since police are symbols of society's laws restricting behavior, maintaining legitimacy within the community is considered essential to the social order.

Evidence suggests that police spend roughly 80% of their time in a symbolic capacity. Decker, Smith and Uhlman (1979) argue that, if police fail to supply this support, it has serious consequences for the community.

The events surrounding the creation of DATTA strongly indicate that policy makers and law enforcement officials were concerned with reassuring the high-technology community that their interests were being considered. The evidence suggests that symbolic reassurance, though not an expressed objective or goal, was a motivating element in DATTA's founding.

Summary

DATTA was perceived by its founders as a practical solution to the problem of high-technology crime. The project addressed the major issues that were perceived as inhibiting investigations and prosecutions. If DATTA were to prove successful, it would be the model for a future state-wide program.

The District Attorney's Technology Theft Association:
Its Implications For Public Policy

Introduction

The DATTA project was an attempt by state and local policy makers to fashion an county-wide campaign against high-technology crime. Its goal was to curb the spread of high-technology crime through law enforcement intervention. To accomplish this goal the following objectives were established:

1. Educate the law enforcement community about the issue of high-technology crime and train them in the latest investigative techniques;
 2. Reduce the amount of jurisdictional fragmentation and increase communication links between law enforcement and the private sector;
 3. Increase the level of crime reporting among victims of high-technology crime; and
 4. Reassure the electronics industry that law enforcement is responsive to their needs.
- (Project Summary, 1985, p. 1)

These objectives were considered crucial to forging a comprehensive program. This section will examine the DATTA

project's success in meeting these objectives and its potential for satisfying the future concerns of policy makers and the public.

DATTA's Impact on The Investigation of Computer Crime,
Semiconductor Theft, and Trade Secret Theft

The training of local law enforcement personnel on the techniques of high-technology crime investigation was provided through the presentation of 20 monthly meetings and five intensive training seminars. The seminars ranged from one to five days, and covered the following topics (R. Elliot, personal interview, September 21, 1987):

- a) introduction to computer crime;
- b) obtaining and utilizing experts;
- c) the problem of semiconductor chip theft;
- d) methods of infiltrating the grey market;
- e) trade secret theft and trade secret laws; and
how to coordinate efforts between
jurisdictions.

These meetings and seminars were held in conjunction with the Industrial Security Managers Group (ISMG), and were conducted at local electronics companies.

DATTA was predicated on the theory that the training of investigators in such high-technology crimes as computer crime, semiconductor chip theft, and trade secret theft would significantly

raise the level of investigations and prosecutions (R. Elliot, personal interview, September 21, 1987). According to Deputy District Attorney Douglas Southard (personal interview, 1986), this premise was proven correct. Between 1980 and 1983, the Santa Clara County District Attorney's Office prosecuted an average of four high-technology crimes a year. By 1987, three years after DATTA's founding, they were averaging 107 cases (Progress Report, 1986). These cases involved violations of California Penal Code Sections 502 and 499c, which deal explicitly with computer crime and trade secret theft.

Table 1
Impact of DATTA Project on Criminal Processing

	Evaluation Periods		
	<u>1/81-1/82</u>	<u>3/85-2/86</u>	<u>3/86-2/87</u>
Total Cases	4	100	114
Number of Convictions	n/a	26	24

Source: (Southard, personal interview, May 5, 1986; Annual Report to the Legislature, 1987, p. 10)

Current DATTA director Ken Rosenblatt (personal interview, April 3, 1989) states that the increase in the number of

high-technology crime cases filed was directly related to the presence of better-skilled investigators. This is supported Jay Bloombecker of the National Center on Computer Crime Data (personal interview, April 4, 1989), who conducted research on disparities between New York and Pennsylvania in computer crime prosecutions. In the year studied, New York had ten prosecutions under its new computer crime law while Pennsylvania had 485. From his interviews Bloombecker determined that the major reason for this difference was the level and quality of training. He argues that it is not enough to just provide new laws; investigators and prosecutors must be properly prepared to apply them.

Along with the increase in investigations came a corresponding rise in the number of convictions. Between 1985 and 1987, the Santa Clara County District Attorney's Office achieved a 23% conviction rate for all high-technology crime. Though comparisons are tenuous, a conviction rate over 20% for any category of property crime is considered above average by most law enforcement standards (R. Elliot personal interview, September 21, 1987). This figure compares favorably with information collected by the Vera Institute of Justice (1977). In a study of criminal cases in New York City, Vera researchers found that only 15% of all criminal investigations lead to a conviction.

According to researchers, if police have the ability to gather tangible evidence, the strength of a criminal case is greatly enhanced (Forst, 1977). This factor is one element that makes

specialized training in high-technology crime so vital (D. Parker, personal interview, May 22, 1986). For example, Carver (personal interview, May 23, 1986) states that, based on his experience, obtaining evidence in computer related crimes is one of the most difficult challenges that confronts an investigator. However, because of the knowledge and skills provided by DATTA's training program, he no longer feels any trepidations about launching a computer crime investigation. In addition, he asserts that he now conducts investigations in both semiconductor chip theft and trade secret theft.

According to Rosenblatt (personal interview, April 3, 1989), as a result of DATTA each jurisdiction in Santa Clara County now has at least one investigator capable of managing a high-technology crime investigation (P. Moore, personal interview, July 12, 1986). For instance, when the large chip theft occurred at Monolithic Memories in 1980, the City of Sunnyvale Department of Public Safety's investigators were not equipped to handle it. Now, the City of Sunnyvale has two highly competent high-technology crime investigators (P. Moore, personal interview, June 12, 1986).

The investigation process was further strengthened by the participation of private-sector volunteers. As Parker (personal interview, May 22, 1986) notes, the use of experts with a knowledge of high-technology is critical to many investigations. According to Southard (personal interview, May 5, 1986), numerous individuals from the private sector have volunteered to provide

technical assistance to DATTA-trained investigators. Rosenblatt (personal interview, April 3, 1989) believes that the increase in available volunteer experts is due to the growing perception among industry personnel that law enforcement is now serious about high-technology crime and that the expert's time will be properly utilized.

The effectiveness of DATTA in improving the investigative proficiency of law enforcement was noted in a 1987 survey of advisory board members:

One board member reported that, in his jurisdiction, they are able to prosecute cases they would have shown no interest in five years ago. The Sheriff's office reported that the project has enhanced their ability to successfully track, investigate, and convict violators ...

Although comments revealed programmatic areas that require refinement, overall comments by advisory board members indicated that the project was successful in enhancing high-technology theft investigation; in strengthening communication links between the respective groups involved; and in enhancing arrest and prosecution efforts in high-technology crime in Santa Clara County. ((Office of Criminal Justice Planning, 1987, p. 11).

It is apparent that DATTA's training increased the ability and willingness of law enforcement personnel to conduct

high-technology crime investigations. Information from the Santa Clara County's District Attorney's Office shows that DATTA produced a noticeable increase in high-technology investigations and successful prosecutions. Interviews with DATTA participants assert that this was directly attributable to better training.

DATTA's Impact on Jurisdictional Fragmentation

DATTA's ability to break down jurisdictional barriers was dependent upon its capacity to bring all the necessary elements together in a cooperative manner. According to Moore (personal interview, July 6, 1986), DATTA project director Robert Elliot was able to organize key law enforcement agencies through strong personal leadership. Prior to DATTA, Elliot was a police captain for the City of Palo Alto Police Department. Moore states that Elliot's law enforcement background gave him immediate credibility with the law enforcement establishment, which tends to be suspicious of non-police personnel.

Elliot's efforts to galvanize the multiple local agencies was aided by the project's placement in the Santa Clara County District Attorney's Office. The District Attorney's office is the only local criminal justice agency with county-wide responsibility. Though it cannot dictate law enforcement policy, it has significant symbolic influence with local police departments due to its prosecutorial role (D. Southard, personal interview, May 13, 1986).

According to Southard (personal interview, May 13, 1986), the participation of each jurisdiction was achieved through vigorous advocacy by principals Elliot and himself. DATTA staff met personally with police personnel to offer information about the program and its importance to the community. To mobilize support among the various organizations, DATTA established an advisory board comprised of influential representatives from selected agencies throughout the county. Through this effort, DATTA was able to convince all 14 local jurisdictions to commit at least one investigator to the project (R. Elliot, personal interview, September 21, 1987).

DATTA organizers fashioned the project as a cooperative effort with the electronics industry by organizing monthly meetings with the ISMG (J. Hacker, personal interview, August 11, 1986). According to Elliot (personal interview, 21, 1987) the participation of this group was crucial since it provided a communications link with the electronics industry. Through this linkage, DATTA was able to gain support and enhance its credibility within the private sector. This support was demonstrated by the electronics industry's willingness to contribute facilities, personnel, and equipment (W. Dexter, personal interview, April 21, 1986). Through the ISMG's involvement, lingering doubts about the private sector's support for law enforcement intervention were substantially allayed (D. Southard, personal interview, May 5, 1986). According to DATTA's 1985/86 progress report:

The participation by high-tech industry representatives in DATTA training seminars has been outstanding. During the first year of the project, 51 industry representatives have donated their time and effort to train, provide facilities and contribute all that it takes to present quality training seminars. (Office of Criminal Justice Planning, 1986, p.4)

Due to the mutual efforts of the ISMG and DATTA, cooperative networks between law enforcement and industry were fostered. "Everyone now knows each other and training assistance is freely provided without hesitation" (J. Hacker, personal interview, August 13, 1986).

Between 1984 and 1987, DATTA conducted 20 meetings and five seminars. The meetings were attended by investigators who represented all the local law enforcement agencies in the county, including state and Federal. These individuals were designated by their departments as a high-technology crime specialist (K. Rosenblatt, personal interview, April 3, 1989). According to Elliot (personal interview, September 21, 1987), the meetings were instrumental in promoting cooperation between all the different law enforcement organizations and agencies. By creating a mutual focus on high-technology crime, DATTA instilled a sense of "mission and teamwork" (Elliot).

William Carver, the City of Santa Clara Police Department (personal interview, May 5, 1986) states that, the investigative process was expedited by personal interaction between agency and

private sector personnel. He states that the initial reluctance of agencies in Santa Clara County to engage in cooperative efforts has diminished significantly. Carver attributes this to the informal networks that evolved through DATTA's small group meetings saying, "Through these meetings you were able to get to know the person in the neighboring jurisdiction on a first name basis. When a situation arose you knew exactly who to call."

Sergeant Pat Moore (personal interview, July 12, 1986) of the Santa Clara County Sheriff's Department states that, since DATTA, he has never "witnessed such cooperation between the different elements of law enforcement than in the area of high-technology crime."

The use of informal networks and mutually-focused groups as a means to foster cooperation and communication is supported by a number of experts. Agent William Filben (personal interview, September 15, 1986) of the California Department of Justice, states that the DATTA project was well structured for achieving its goal of reducing interjurisdictional fragmentation. According to Filben, "A group of law enforcement people focusing on one area will always augment cooperation and communication. A common focus and close interaction breaks down artificial barriers."

As a result of its training seminars and small group meetings, the DATTA project lessened interagency fragmentation, which previously had inhibited the investigation of crimes that transcended jurisdictional boundaries (K. Rosenblatt, personal

interview, April 3, 1989). For example, "The sheriff's office reported that participation in the DATTA project has facilitated a cohesive working relationship among all facets of law enforcement that have chosen to become a part of the DATTA team" (Office of Criminal Justice Planning, 1987, p. 11).

According to Carver (personal interview, May 5, 1986) the networks will continue to evolve as long as the meetings are kept small and informal. It is through this informal interaction that cooperation and communication are promoted.

DATTA's Effect on Reporting Rates

Many experts and practitioners assume that the electronics industry's reluctance to report high-technology crime is primarily due to the lack of coordination between industry and local police (Beguai, 1978). For instance, in DATTA's 1987 annual report to the legislature it was noted that:

The lack of coordination between industry and law enforcement contributes to non-reporting of high-technology crime. Non-reporting of crime is a major stumbling block to the development of a crime prevention strategy. (Office of Criminal Justice Planning, 1987, p. 15)

Therefore, one of DATTA's primary objectives was to raise the level of high-technology crime reporting.

To determine the basis for the electronics industry's failure to report crime, DATTA distributed a questionnaire to a random sample of 243 high-technology companies. Of the 97 respondents, the reason for not reporting crimes to the police in 68% of the cases was because the loss was considered insignificant. In another 28% of the cases, it was noted that reporting would be a waste of time. In 13% of the incidents, companies reported that they feared negative publicity. In only 7% of the cases was the lack of law enforcement assistance cited as a primary reason for not reporting high-technology crime (see graph).

Figure 1

Reasons for Not Reporting Instances of High-Technology Crime
(97 respondents out of 243 polled)

Source: Annual Report to the Legislature, 1987, p.10

According to information from the Santa Clara County District Attorney's Office, only 38% of high-technology crimes are ever reported to the police (Office of Criminal Justice Planning, 1987). It is believed that this low degree of reporting is partially responsible for the inability of law enforcement to build a viable deterrent (R. Elliot, personal interview, September 21, 1987).

Table 2
Reasons for not Reporting Instances of High-Technology Crime

Number of high-technology Crimes Reported to Police N = 1,130	
Number Reported to Police	Percent of Reported HT Crimes
432	38%

Source: Annual Report to the Legislature, 1987, p.14

Despite the efforts of DATTA, the reporting rates for high-technology crime in Santa Clara County as presently measured, reveal that they are consistent with reporting rates for all forms of crime from around the nation. Victimization surveys have consistently shown that only 35% of all domestic crimes are ever reported to the police (Harlow, 1985). According to Southard (personal interview, May 13, 1986) the current rate of reporting

makes building a viable deterrent extremely difficult. He states that although DATTA's results have been impressive, the current reporting rates are insufficient and will not impact crime rates.

The fact that only a small percentage of DATTA's survey respondents cited the lack of law enforcement responsiveness indicates that police performance is not the major reason for under-reporting. According to Parker (personal interview, May 22, 1986) better police response will only marginally raise reporting rates. This is because companies are more concerned with additional financial losses and negative publicity than they are with criminal apprehension. Therefore, the objective of significantly increasing reporting rates through law enforcement action may be unrealistic.

DATTA and The Deterrence Effect

The concept of deterrence involves two objectives: general deterrence and specific deterrence. Through general deterrence, the criminal impulse is tempered by the perceived risk of apprehension. Specific deterrence occurs when the individual offender is discouraged from repeating criminal acts after experiencing criminal sanctions (Currie, 1985).

Law enforcement intervention tends to have the greatest deterrent impact on first time white-collar offenders. First time white-collar offenders generally have strong community and family ties and are therefore more threatened by the social stigma

associated with criminal prosecution (Johnson & Douglas, 1978). Since most high-technology crimes are perpetrated by white-collar professionals, increased levels of law enforcement should theoretically decrease the level of crime.

Research by Donn Parker at SRI International (personal interview, May 22, 1986) found that law enforcement intervention with individual first-time, professionally employed computer criminals has a specific deterrent effect. Parker conducted random interviews with 30 convicted computer criminals out of a total of a thousand cases compiled by SRI since 1958. Out of those interviewed only one committed a subsequent offense.

Based on the information he collected, Parker (1983) concluded:

Most of the famous computer criminals of the past have overcome their problems and developed new and better legitimate careers for themselves. None of them has returned to criminal activities as far as is known.

Amateur white-collar computer criminals interviewed so far seem to demonstrate that this type of criminal is not recidivistic. (p. 94)

Though no recidivism study has been completed on convicted high-technology offenders in Santa Clara County, Elliot (personal interview, May 13, 1986) states that many of the offenders he has seen share the same profile as Parker's sample. He therefore

believes that DATTA is successful in deterring the first-time, professionally-employed, high-technology offender.

Although there is evidence that suggests a specific deterrent effect for non-career white-collar criminals, there is a growing indication that the profile of high-technology criminals is changing. According to Bloombecker (personal interview, April 4, 1989), the availability of high-technology is resulting in more people having access to technology who are not professionally-employed and in many cases are career criminals. This is confirmed by Mr. William Baker (personal interview, March 29, 1989) of SRI International, who states that recent data indicates that certain types of high-technology offenders, such as "hackers", are showing high recidivism rates when compared to a decade ago when they were more likely to be employed by the company they victimized.

General deterrence is a function of the degree of fear among potential offenders of the possibility of being caught. If the belief is present that police actions are effective and certain, then the crime rate will decrease. For example, Greenwood, Chaiken, and Petersilia (1977) concluded from their research that criminal investigations deter potential criminal conduct. According to Greenwood, Chaiken, and Petersilia (1977):

The process of carrying out an investigation (whether successful or not) presumably has in itself some deterrent value, even though that is not its primary purpose. In the extreme, it must be assumed that if no investigations were

ever conducted, crime rates would increase, although we have no way of estimating at what rate. This effect applies also to individuals who have not committed crimes but who assume that, if they did, there would be an investigation. (p. 30)

Prior to DATTA, there was very little police involvement in high-technology crime. However, because of DATTA, there is now a growing perception among high-technology personnel that local police agencies now consider these crimes serious (J. Hacker, personal interview, September 11, 1986). In addition, the police have managed to foster a more competent image within the high-technology community. Parker (personal interview, May 22, 1986) states that this is critical since one reason why people engage in high-technology crime is because they perceive the risk of detection and apprehension to be low. By adopting a more determined image, police are communicating to the potential offender that these crimes will carry a risk.

Because it is impossible to estimate what the rate of high-technology crime in Santa Clara County was prior to DATTA, there is no accurate means to measure DATTA's general deterrent effect. However, present evidence from criminal justice literature indicates that merely increasing the presence of law enforcement does not produce a general deterrent effect. For example, according to a study by The President's Commission on Law Enforcement and Administration of Justice (1967), there is no evidence to show that increasing the resources of police significantly affects crime rates.

The Commission found that in the various cities they studied there was no relationship between the number of reported crimes and the number of police.

DATTA and Symbolic Reassurance

According to private sector security managers, DATTA heightened the level of confidence in the police (M. Zitke, personal interview, 1986). Many experts feel that this is an important, but overlooked consideration for law enforcement policy. According to Decker, Smith, and Uhlman (1979):

Preventing crime and apprehending criminals are, of course, primary goals of a police force. But to assess performance by this single standard is to discount many other services which police departments provide, services which help to maintain order but contribute only indirectly to crime control. It is our contention that both police and the public would benefit if the criteria for evaluating performance were broadened to include other activities. (p. 53)

Based on interviews with law enforcement personnel and private sector security managers, prior to DATTA, there was a pervasive lack of confidence in the law enforcement community's ability to respond to high-technology crime. According to Hacker (personal interview, April 13, 1986), DATTA was highly effective

in promoting the image of law enforcement and therefore enhancing its legitimacy among the private sector community.

By diverting resources and maintaining a high profile among the high-technology community, DATTA was able to quell many of the grievances that were previously expressed. In responding to community pressure, DATTA altered unfavorable perceptions and restored an element of confidence in the police and public policy makers (K. Rosenblatt, personal interview, April 5, 1989).

Public Policy Considerations

A study of the DATTA project highlights some emergent observations. A number of these observations are of particular significance to public policy makers.

- First, based on interviews with DATTA participants and a review of the research, a small select number of investigators meeting on a regular basis will improve the professional cooperation between law enforcement jurisdictions in the investigation of high-technology crime cases. This is an important accomplishment within a bureaucracy that is notorious for its lack of interjurisdictional cooperation.
- Second, it appears that DATTA eliminated the "avoidance syndrome" among law enforcement personnel with respect to high-technology crime. According to information from the Santa Clara County District

Attorney's Office, DATTA resulted in a significant increase in the number of investigations and convictions. The training resulted in at least one trained investigator within each of the County's 14 jurisdictions.

- Thirdly, DATTA improved the relationship between the private sector and law enforcement (J. Hacker, personal interview, September 11, 1986). Through a cooperative linkage, industry donated personnel and equipment to the effort. In addition, there is now a core of expert volunteers from the private sector who stand ready to assist the police during criminal investigations (Southard, personal interview, May 13, 1986).
- Fourth, there is no substantial evidence that DATTA was able to effect the crime reporting habits of industry. Theoretically, without higher levels of crime reporting, a viable deterrent cannot be established. General deterrence in high technology crime is dependent on the commitment of industry to promptly report crime to the police to allow immediate intervention. Although DATTA brought about an increase in investigations and prosecutions, there is no indication that it led to a higher volume of crime reporting. Crime reporting rates are linked to other elements and considerations that are beyond the reach of law enforcement policy. Therefore,

the goal of reducing crime rates solely through law enforcement intervention may be unreachable.

- Fifth, there is currently no evidence to demonstrate that increasing the amount of resources available to law enforcement will reduce crime rates. Though there is some indications that law enforcement intervention may have a specific deterrent effect with individual first-time white-collar offenders, many experts argue that the spread of high-technology will result in more high-technology crime by career criminals.
- Finally, for policy makers seeking to enhance law enforcement's image among the high-technology community, DATTA was effective (J. Hacker, personal interview, August 11, 1986). The notion of symbolic reassurance is an often overlooked issue since it does not produce tangible or measurable results. However, criminologist believe that it is essential for the preservation of public order for policy makers to maintain the integrity of their law enforcement agencies.

Future Research Considerations

The study of high-technology crime is still in its infancy and there is little substantive or conclusive information available.

Researchers interested in pursuing this approach to crime prevention and containment should consider the following issues.

There is presently a dearth of information on the actual amount of high-technology crime. Most of the information available is unreliable and incomplete. For example, the problem was expressed in DATTA's 1987 annual report to the legislature:

Due to the nature of high-technology industry, it is difficult to collect crime statistics. There is a lack of knowledge regarding the causes and scope of high-technology crime. Currently, no successful method had been developed to collect high-technology crime statistics at the local level. There is no coordinated attempt to devise a cohesive method to collect statistics. (Office of Criminal Justice Planning, 1987, p. 15)

Until a method is devised for gathering adequate information, conclusions about the range and effect of high-technology crime will remain mainly estimates.

An area of criminal justice research that has not been closely examined is the relationship between police actions on white-collar high-technology crime rates. As Brintall (1979) points out:

Little attention has yet been given to ways in which police patrol practices can be employed as a means of detecting white-collar crime or ways in which police detectives can be trained and deployed to conduct or assist in white-collar crime investigation. Evidence suggests that police detectives

may even be more effective in this area than more traditional roles. (p. 47)

Although there is a basis to support the belief in a specific deterrence effect among first time white-collar high-technology offenders, there is a need to examine how extensive it is and what policies can best exploit it.

Conclusion

As high-technology crimes increase, policy makers are seeking to craft policies that will address these problems. The DATTA project provides one of the first opportunities to examine the possible effects of law enforcement intervention in this area. DATTA was designed to overcome the major obstacles that were impairing the law enforcement community's ability to respond to high-technology crime.

Evidence from the DATTA project indicates that better training will lead to more arrests and convictions, and will improve interjurisdictional cooperation. In addition, it appears that the average professional white-collar high-technology offender is unlikely to reoffend once apprehended. However, there is no evidence that a general deterrent effect will result solely by augmenting the resources of police. Although DATTA-trained investigators did conduct more investigations, there was no significant increase in the willingness of companies to report

crimes. This issue appears intractable and will likely continue to limit the potential impact of law enforcement intervention.

Policy makers, in designing solutions to high-technology crime, may have to lower their expectations about substantially reducing crime rates strictly through law enforcement. However, based on the evidence from DATTA, it appears that the program was effective in improving the investigative process, reducing jurisdictional fragmentation, creating a specific deterrence effect with first time offenders, and maintaining public confidence in law enforcement agencies. Though more research is needed about the causes and solutions to high-technology crime, it appears that the DATTA model could be one element to a more comprehensive approach.

References

- American Bar Association. (1984). Task force on computer crime survey. Washington, D.C.: author.
- Bequai, August. (1978). Computer Crime. Massachusetts: Lexington Books.
- Bloombecker, Jay. (1986). First annual statistical report of the national center for computer crime DATTA. Los Angeles, CA: Author.
- Brintall, Michael. (1979, Spring). Entrepreneurship in the local prosecution of economic crime. Policy Studies, 7, p. 47.
- Cira, John. (1983, September). Computer abuse: The silicon pry bar. The Police Chief, pp. 46-47.
- Computer sting nets seven juveniles. (1985, July 6). New York Times, p. 17.
- Conklin. (1981). Criminology. New York: MacMillan Publishing Co., Inc.
- Currie, Elliot. (1985). Confronting crime: Why there is so much crime in America and what we can do about it. New York: Pantheon Books.
- Fisk, Robert B. (1976). Crimes against business. Proceedings of Seminars Held in New York, NY, (pp. 33-34). Washington, D.C.: U.S. Department of Commerce.

- Forst, B., Fucianovic, J. & Cox, S. (1977). What happens after arrest? A court perspective of police operations in the District of Columbia. Washington, D.C.: Institute of Law and Social Research.
- German hackers break into NASA network. (1987, September 16). New York Times, p 14.
- Greenwood, Peter W., Chaiken, Jan M. & Petersilia, Joan. (1977). The criminal investigation process. Massachusetts: O.C. Heath and Company.
- Harlow, Caroline W. (1985, December). Reporting crimes to the police. Washington, D.C.: Bureau of Justice Statistics, National Institute of Justice.
- Industrial Security Managers Group. (1980). Organizational Objectives. Unpublished paper.
- Jacob, Herbert. (1984). The frustration of policy: Response to crime by American cities. Massachusetts: Little Brown and Company.
- Johnson, John & Douglass, Jack. (1978). Crime at the top. San Jose, CA: J.B. Lipponcott Company.
- Kaye, Jeff. (1982, October 3). Finkelstein calls for Federally funded task forces. San Jose Mercury News, p. 1B.
- Kaye, Jeff. (1983, January 13). D.A. establishes special operations units. San Jose Mercury News, p. 1B.
- Krause, Leonard I. & MacGakan, Ailun. (1979). Computer fraud and countermeasures. New Jersey: Prentice Hall, Inc.

- Markoff, John. (1987, July 24). Computer expert warns of threats from hacker. San Francisco Examiner, pp. 1, 2C.
- Markoff, John. (1987, December 20). Vandals hit computers with virus. San Francisco Examiner, pp. 1, 16.
- Masuda, Yengi. (1981). The information society. Washington, D.C.: World Future Society.
- Maxfield, John T. (1985). Computer bulletin boards and the hacker problem. Southfield, MT: Boardscam.
- Moulton, Rolf. (1983, September). Computer abuse: a multidisciplinary investigative approach. The Police Chief, pp. 48-49.
- Naisbitt, John. (1984). Megatrends. New York, New York: Warner Books.
- Nycum, Susan H., Snow, Gaston, Bartlett, Eby, Parker & Vonn, B. (1985, February). Prosecutorial experience with state computer crime laws. SRI International, p. 6.
- Office of Criminal Justice Planning. (1986). Progress report: District Attorneys Technology Theft Association. Sacramento, CA: State of California.
- Office of Criminal Justice Planning. (1987, February). High technology crime prevention program: Annual report to the legislature. Sacramento, CA: State of California.
- Parker, Donn. (1983) Fighting computer crime. New York: Charles Scribner Sons.

- Parker, Donn. (1986). New concepts for information security.
Unpublished manuscript.
- The President's Commission on Law Enforcement and Administration
of Justice. (1967). The challenge of crime in a free society.
Washington, D.C.: U.S. Government Printing Office.
- Rogers, Everett M. & Larsen, Judith K. (1958). Silicon valley fever:
Growth of high-technology culture. New York: Basic Books, Inc.
- Santa Clara County District Attorney's Office. (1986). Project
Summary. San Jose, CA.: Author
- Santa Clara County sting. (1984, November). Computer Crime
Digest, p. 9.
- Schgolberg, Stein. (1983). Computers and penal legislation.
Norway: Norwegian Research Center for Computers and Law.
- Schrage, Michael. (1985, August 12). No peeking in my computer.
The Washington Post, p. 5.
- "Silicon valley" D.A. forms multi-agency task force to combat high
tech thefts. (1983, May). Computer Crime Digest, 3.
- Simon, Herbert A. (1957). Administrative Behavior. New York: The
Free Press.
- Southard, D. (1982, May). Transfer of United States high technology
to the Soviet Union and Soviet bloc nations. Hearings Before the
Permanent Subcommittee on Investigations of the Committee on
Governmental Affairs, United States Senate, Ninety Eighth
Congress, pp. 143-154.

- Spears, Gregory. (1985, September 12). Social security computer fraud: System is easy mark for insiders, report says. San Jose Mercury News, p. 13.
- State of California. (1984). High technology crime prevention program (Assembly Bill No. 1078). Sacramento, CA: State of California.
- Stein, Richard H. (1981). Determining liability for infringement of mask work rights under the semiconductor chip prohibition act. Minnesota Law Review, 20, 1039.
- Swartz, Herbert. (1982, October). Taking the bite out of computer crime. Business Computer Systems, pp. 45-46.
- Sweitzer, James A. (1986). Computer crime and business information. New York: Elsevina.
- Vera Institute of Justice. (1977). Felony arrests: Their prosecution and opposition in New York City's courts. New York, NY: Author.
- Vogyves, Mary R. (1980). The investigation, prosecution, and prevention of computer crime: A state-of-the-art review. Computer Law Journal, Spring, p. 395.
- Yates, Douglas. (1977). The ungovernable city. Cambridge, MA: MIT Press.