U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

National Institute of Justice / *Issues and Practices*

Organizing for Computer Crime Investigation and Prosecution

About the National Institute of Justice

The National Institute of Justice is a research branch of the U.S. Department of Justice. The Institute's mission is to develop knowledge about crime, its causes and control. Priority is given to policy-relevant research that can yield approaches and information that State and local agencies can use in preventing and reducing crime. The decisions made by criminal justice practitioners and policymakers affect millions of citizens, and crime affects almost all our public institutions and the private sector as well. Targeting resources, assuring their effective allocation, and developing new means of cooperation between the public and private sector are some of the emerging issues in law enforcement and criminal justice that research can help illuminate.

Carrying out the mandate assigned by Congress in the Justice Assistance Act of 1984, the National Institute of Justice:

- Sponsors research and development to improve and strengthen the criminal justice system and related civil aspects, with a balanced program of basic and applied research.
- Evaluates the effectiveness of justice improvement programs and identifies programs that promise to be successful if continued or repeated.
- Tests and demonstrates new and improved approaches to strengthen the justice system, and recommends actions that can be taken by Federal, State, and local governments and private organizations and individuals to achieve this goal.
- Disseminates information from research, demonstrations, evaluations, and special programs to Federal, State, and local governments, and serves as an international clearinghouse of justice information.
- Trains criminal justice practitioners in research and evaluation findings, and assists practitioners and researchers through fellowships and special seminars.

Authority for administering the Institute and awarding grants, contracts, and cooperative agreements is vested in the NIJ Director. In establishing its research agenda, the Institute is guided by the priorities of the Attorney General and the needs of the criminal justice field. The Institute actively solicits the views of police, courts, and corrections practitioners as well as the private sector to identify the most critical problems and to plan research that can help solve them.

James K. Stewart
Director

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

Organizing for Computer Crime Investigation and Prosecution

by

Catherine H. Conly

July 1989

Issues and Practices in Criminal Justice is a publication series of the National Institute of Justice. Designed for the criminal justice professional, each *Issues and Practices* report presents the program options and management issues in a topic area, based on a review of research and evaluation findings, operational experience, and expert opinion in the subject. The intent is to provide criminal justice managers and administrators with the information to make informed choices in planning, implementing and improving programs and practice.

Prepared for the National Institute of Justice, U.S. Department of Justice, by Abt Associates Inc., under contract #OJP-86-C-002. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

National Institute of Justice
James K. Stewart
Director

Program Monitor

Johnathan Budd
National Institute of Justice
Washington, D.C.

The Assistant Attorney General, Office of Justice Programs, coordinates the activities of the following program Offices and Bureaus: the Bureau of Justice Statistics, National Institute of Justice, Bureau of Justice Assistance, Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime.

Foreword

With the virtual explosion of technological advances in the 1980's, computers and their applications have become an integral and indispensible part of our society and its institutions. Computers were found in one home in a hundred at the beginning of the decade — by 1987 one in five households had them. Today they are as common a business tool as the ledger or the cash register. Given this dramatic increase in the use and accessibility of computers in the home and in business, it is not surprising to see an increase in the use of computers in the commission of crime.

Law enforcement faces new challenges as it seeks to strengthen capabilities for successfully investigating and prosecuting computer crime into the 1990's. Use of computers has proliferated not only in traditional crimes of theft such as embezzlement and fraud; increasingly, drug rings, prostitution rings, child pornographers and pedophiles have turned to computers to facilitate their illicit operations just as legitimate businesses do. Police say they arrive at the scene of these criminal networks and discover computers in operation.

Detectives and prosecutors realize that if law enforcement is to make greater inroads in investigating and prosecuting these types of cases, they need to become conversant with computer operations. In fact, the 1986 National Assessment Program Survey conducted by the National Institute of Justice found that 65 percent of the police chiefs and sheriffs sampled considered approaches for handling computer crime to be a high priority for further research and information sharing.

As part of its response to this need, the National Institute of Justice has published this *Issues and Practices* report, which provides an overview of existing approaches agencies are using to handle computer-related crime cases, illustrative case examples of crimes investigated by state and local personnel, and recommendations for effective investigation and prosecution of computer crime.

Two companion volumes, *Computer Crime: Criminal Justice Resource Manual* and *Dedicated Computer Crime Units*, are other important parts of NIJ's effort to provide information and ideas that law enforcement can use in meeting the challenges posed by computer crime.

The proud history of law enforcement in the United States has been marked by a remarkable capacity to successfully confront and overcome new challenges. With the publication of these volumes, the National Institute of Justice hopes to assist law enforcement and prosecutorial efforts to meet the challenges they face combating crime in the computer age.

James K. Stewart
Director
National Institute of Justice

Acknowledgements

Many organizations and individuals made significant contributions to this report. Without the participation of a number of law enforcement and prosecutors' agencies, it would have been impossible to describe the current trends in local and state investigation and prosecution of computer-related crime. Special thanks, therefore, are due the following agencies that allowed me to spend considerable time with members of their staffs:

Baltimore County, Maryland
Police Department
Economic/Computer Crime Unit
Investigator Frank Simmons
Investigator Calvin Lane

Columbus, Ohio Police Department
Organized Crime Bureau
Officer Robert M. Snyder

Franklin County, Ohio
Prosecuting Attorney's Office
Economic Crimes
Asst. Prosecuting Atty. Robert Smith
Asst. Prosecuting Atty. Daniel Abraham

Jefferson County, Colorado
Sheriff's Office
Criminalist William F. Chapman, Jr.

Lakewood, Colorado
Police Department
Intelligence Division
Detective Larry L. Scheideman

Maricopa County, Arizona
Sheriff's Department
Technical Crimes Investigation
Sergeant William Nibouar

Office of the Attorney General,
Arizona
Asst. A.G. Gail Thackeray

Philadelphia, Pennsylvania
Police Department
Economic Crime Unit
Detective Philip J. Silverman
Detective Michael J. Mullen

Philadelphia, Pennsylvania
District Attorney's Office
Economic Crimes
Asst. D.A. James Fitzpatrick
Forensic Accountant Mickey Litt

Many other individuals have shared their time and expertise. A number served on a special advisory panel to this project. Among them are Mr. James Caruso, AT&T Corporate Security, Warren, New Jersey; Mr. Wayne Cerow, Cerow Investigations and Consultants, Phoenix, Arizona; Mr. Robert J. Humphreys, attorney with McCardell, Downelly, Bensen, Ahern, P.C., Virginia Beach, Virginia; Mr. Donn B. Parker, SRI International, Menlo Park, California; and Mr. Edward Rapacki, Middlesex County Massachusetts District Attorney's Office. A number of others met with me and shared their particular expertise. I am grateful for the time contributed by Mr. Anthony Adamski, Jr., Federal Bureau of Investigation, Washington, D.C.; Judge H.

Jeffrey Bayless, Denver, Colorado; the members of the Colorado Association of Computer Crime Investigators; Dr. James Conser, Youngstown State University, Columbus, Ohio; Mr. Jim Graham, assistant State's Attorney, Brevard County, Florida; Mr. Ken McLeod, private investigator and computer security specialist, Buckeye, Arizona; Mr. Daniel J. Piskur, Security Administrator, CompuServe, Inc., Columbus, Ohio; Special Agent Stephen R. Purdy, United States Secret Service, Washington, D.C.; and Professor John T. Soma, University of Denver Law School.

The project was guided with great thoughtfulness by Mr. Jonathan Budd, a member of the National Institute of Justice's (NIJ) Research Applications and Training Division and supported strongly by Ms. Virginia Baldau, Division Director, and Mr. Paul Cascarano, Assistant Director of NIJ.

Finally the contributions of three employees of Abt Associates Inc. deserve acknowledgement. Special thanks are due Ms. Susan McWhan, who helped organize a number of materials for this report and was instrumental in developing the list of reference materials provided at the end and preparing materials for several of the appendices. Acknowledgement is also due Dr. Jan Chaiken, who contributed many helpful suggestions to the several drafts of this report. I would like to thank Ms. Kris Mattson who carefully guided the production and printing of this document.

Table of Contents

Chapter I: Introduction

With the proliferation of computers in our society, the issues and problems surrounding computer-related crime continue to grow as well. Already a large component of white-collar crime, computer-related crime is increasing rapidly in rate, seriousness, and sophistication. While it is difficult to determine the exact incidence of computer-related crime or the total economic losses associated with it, computers have been involved in recent years in crimes of unprecedented economic cost, from electronic funds transfer fraud to inventory loss.

As computer-related crime proliferates, state and county prosecutors face an increasing demand for prosecution strategies and technical expertise in this expanding area. In some cases, local prosecutors will need to work cooperatively with federal prosecutors, addressing cases with both intrastate and interstate aspects; in other instances, computer-related crimes will have a purely local impact and be prosecuted under state law. Choice of law and division of investigative responsibility may not always be clearly defined. Existing federal legislation defines several computer-related crimes, but does not clearly specify what agencies or personnel shall have investigation responsibility. Additionally, statutes in 48 states prohibit some form of computer-related crime, either by modification of existing laws (e.g., those pertaining to theft) or, more commonly, in separate computer crime chapters in their criminal codes.[1]

The experiences of criminal justice agencies now responding to the challenge of computer-related crimes demonstrate the importance of developing investigation and prosecution strategies *before* major cases are presented. The following issues highlight this point.

- When a computer-related offense is reported, an agency that has no plan for addressing computer-related offenses may seem unresponsive or incompetent due to its lack of knowledge about the crime. In the time it takes the agency to develop the requisite expertise, offenders may disappear or effectively disguise their criminal activities. Victims will be less likely to report in the future.
- Without trained staff who can assist in the collection of computerized evidence, important evidence may be lost, destroyed, or tainted.
- Agencies that are unaware of the unique need for proactive investigations and prosecutions of computer-related crimes will miss opportunities to develop contacts with the education and business

communities, which may be critical to preventing future offenses, improving reporting of the crime, and developing contacts with computer experts who are often essential to understanding and proving a computer-related case.

Inevitably, as computers become widespread in society, all law enforcement agencies will need to have, or be able to obtain access to, investigators who are familiar with computer-related crime. Prosecutors' offices will need individuals who understand the unique nature of computer evidence and the ways it should be collected and introduced in a successful criminal prosecution. Enlightened law enforcement administrators recognize their needs in this area. In the 1986 National Assessment Program survey, 65% of the police chiefs and sheriffs sampled indicated that handling computer crime was a problem that warranted research and technical assistance.[2]

To help local law enforcement and prosecutors' agencies focus attention on computer-related crime, this report reviews a variety of ways in which agencies are handling the problem. The report highlights the range of existing approaches to computer-related cases, from situations in which a single investigator handles the cases to those involving networks of shared resources or formal computer crime teams. It includes:

- case examples of several computer-related crimes investigated by state and local personnel,
- a review of problems associated with the investigation and prosecution of computer-related crime,
- a discussion of the resources necessary to accomplish the tasks,
- a review of the sources of expert assistance, and
- recommendations for improving the handling of these crimes at the state and local levels, including a set of core elements and options that agencies will need to consider when planning a response to computer-related offenses.

The information in this report was obtained in three phases:

1. Initially, an extensive review of existing literature and news articles on computer-related crime was conducted, both to identify investigation and prosecution trends and to evaluate expert opinion.
2. This was followed by telephone interviews with investigators, prosecutors, victims, researchers, and consultants who have participated in the investigation and prosecution of computer-related crimes. Potential interview subjects were identified through the literature search, through informational calls to law enforcement and prosecutors' offices at the federal, state, and county levels, and by referral (as persons interviewed directed us to others active in the field).

3. Drawing from information gained in the first two phases, four sites were chosen for in-depth study and site visits. Sites were chosen to reflect the range of existing methods for investigating and prosecuting computer-related crimes.

In the course of the study, it quickly became clear that few state and county criminal justice agencies currently have staff available with the background and training necessary to prosecute computer-related crimes. We were able to identify less than 20 sites nationwide that reported any experience with computer-related investigation or prosecution; of these, fewer than half actually dedicated full-time staff members to these activities. While small- and medium-sized offices stated that they had not yet faced an adequate number of computer-related crime reports to justify specialized staff training, even many large offices in cities with significant financial interests reported that they had not yet organized to address the special challenges of computer-based theft. Among those offices currently engaged in computer-related investigations, the number of cases handled annually varies according to agency size and extent of staff commitment, but rarely exceeds 50 cases per year.

While our literature and telephone survey highlighted the need for enhanced and coordinated investigation and prosecution, our site study contributed to an understanding of how small- and mid-sized state and county law enforcement and prosecutors' offices can begin to meet this challenge. In four diverse sites, investigators and prosecutors used a variety of mechanisms to help develop staff expertise and overcome limited resources. These sites included:

Maricopa County, Arizona, surrounding Phoenix, in which the county sheriff's office has a formal, two-person computer crimes unit, and the state Attorney General's office dedicates an assistant attorney general and one investigator to handling computer-related crimes;

Denver and Lakewood, Colorado, where computer-related crimes are most frequently handled by intergovernmental task forces;

Columbus, Ohio, where a single law enforcement officer operates in conjunction with the Franklin County prosecuting attorney's office to process computer-related crimes; and

Philadelphia, Pennsylvania, where two officers in the city's Economic Crime Unit handle computer-related cases as needed.

The report focuses on the range of strategies for investigating and prosecuting computer-related crimes in local and state agencies, emphasizing ways that agencies without existing computer crime units may prepare to investigate and prosecute those offenses. There is limited emphasis on

ways that larger offices may develop comprehensive, specialized computer crimes units. A more detailed description of the operation of dedicated computer crime units is the subject of another study sponsored by the National Institute of Justice (NIJ) entitled, *Dedicated Computer Crime Units.*[3] In addition, readers may wish to consult the recently updated *Criminal Justice Resource Manual,*[4] which includes detailed descriptions of methods used to commit computer-related crimes, types of offenders, detection and prosecution strategies, computer crime laws, and computer technology and terminology.

Endnotes

1. Richard C. Hollinger and Lonn Lanza-Kaduce, "The Process of Criminalization: The Case of Computer Crime Laws," *Criminology*, Vol. 6, No. 1 (1988):104.
2. J. Thomas McEwen and Hugh Nugent, *Results of the National Assessment Survey: Police and Sheriffs*, Research In Action (Washington, D.C.: National Institute of Justice, 1988).
3. J. Thomas McEwen, et al. *Dedicated Computer Crime Units* (Washington, D.C.: National Institute of Justice, 1989).
4. Donn B. Parker, *Computer Crime: Criminal Justice Resource Manual* (Washington, D.C.: National Institute of Justice, 1989).

Chapter II: The Impact of Computer-Related Crimes

Computer-related crimes have a surprisingly wide impact and variety, from sophisticated institutional transactions to the victimization of individuals. Although some offenders are trusted corporate employees without prior records, others may have a history of more typical property and personal crimes, and may simply be using computer access as a potent new tool for achieving criminal goals. Recent law enforcement reports suggest that—just as legitimate business managers have found computers indispensable in conducting business—organized criminals, drug dealers, and even child pornographers increasingly depend on computerized transactions. Additionally, computer-related crimes involving theft or embezzlement do not all involve large and financially sound businesses; in many cases, the victims are the individuals and small businesses that have traditionally been protected by state and county law enforcement.

This chapter describes typical types of computer-related offenders and offenses that may be encountered on the local level. It is not intended to categorize crimes by statutory definition, but merely to acquaint the practitioner with the range and variety of crimes that may occur.

The Typical Computer Criminal

Although computer-related crime may be committed by any person with access to a personal or business computer, certain characteristics appear to be common. According to a noted computer security consultant, the profile of the "typical computer felon" may be described as follows:[1]

- 15-45 years old
- Usually male, although women are increasingly entering the field
- Ranges widely from the highly experienced technician to a minimally experienced professional with little or no technical experience
- Usually no previous contact with law enforcement
- Targets both government and business
- Bright, motivated, ready to accept the technical challenges
- Fears exposure, ridicule, and loss of status with the community

- Majority of cases are one-person shows; however, conspiracies of two or more criminals are surfacing
- Appears to deviate little from the accepted norms of society
- Usually holds position of trust within the company; has easy access to the computer systems
- Usually on guard; is the first to arrive and the last to leave the office; takes few or no vacations
- Justifies criminal acts by viewing them as just a "game".

Terminology

During the past decade there has been considerable debate over the definitions of such terms as computer crime, computer abuse, computer fraud, computer-related crime, high-tech crime, and information crime, among others. For example, efforts to distinguish among computer abuse, computer fraud, and computer crimes have led to the following definitions:

- *Computer abuse* "encompasses a broad range of intentional acts that may or may not be specifically prohibited by criminal statutes. Any intentional act involving knowledge of computer use or technology is computer abuse if one or more perpetrators made or could have made gain and/or one or more victims suffered or could have suffered loss."[2]
- *Computer fraud* is any crime in which a person "may use the computer either directly or as a vehicle for deliberate misrepresentation or deception, usually to cover up the embezzlement or theft of money, goods, services, or information."[3]
- *Computer crime* is any violation of a computer crime statute.[4]

For the purposes of this report, computer-related crime, defined to be any illegal act that requires the knowledge of computer technology for its perpetration, investigation, or prosecution, is used to capture the broad range of offenses that investigators and prosecutors have been required to handle.

Telecommunications Fraud

During the 1970s some individuals defrauded phone companies by using stolen account numbers or reversing charges to pay phones. Those frauds have continued in the 1980s, but changing technology has permitted sophisticated forms of theft of telecommunications services. Moreover, since the changes in technology largely arise from the computerization of the phone industry, these more sophisticated offenses often fit state and federal definitions of computer

crime and require sophisticated investigation and prosecution strategies.[5]

One interesting example of computer-related telecommunications fraud involved the infiltration of a Philadelphia company's voice mail service. Voice mail systems allow callers to leave recorded messages for the owner of what amounts to a telephone mailbox. In a large company the rental of these systems can be quite costly (e.g., $18 per line per month) and the use of the system quite important to the operation of the business. In the Philadelphia case, callers from Arizona used stolen Sprint codes to tap into the company-managed voice mail system and reprogrammed it to exchange information regarding their own illegal business. The callers amassed hundreds of dollars of illegal Sprint calls and blocked company employees from using the voice mail system. After Sprint and the Philadelphia company independently discovered the problems, they asked the Maricopa County, Arizona, Sheriff's office to investigate.

This case illustrates how criminals using stolen codes to communicate with each other can avoid an obvious connection with each other, since the phone bills are sent to the unsuspecting owners of the codes instead of the criminals. This anonymity is especially useful to drug dealers and organized criminals.

Embezzlement

One of the oldest white collar crimes, embezzlement, can be considerably more complex to investigate when it is assisted by computers. Computerized financial transactions can occur entirely within the computer system; tracing the criminal means getting the necessary information and evidence out of the computer.

One embezzlement handled by a former assistant district attorney in Denver, Colorado involved theft from a brokerage firm by one of the firm's agents. The crime involved changing a cash account into a margin account, altering the symbol that represented shares owned, and moving a decimal point. The agent stole $178,000 before the firm accidentally detected the crime.

Several computer-related crimes have involved theft of money from computerized cash registers. One described by Philadelphia detectives involved a department store employee who used the store's cash register, which was tied in to the store's computer system, to clear her own charge account and those of her friends. In that case the store decided not to prosecute.

Computer Hacking

The term computer hacker, in its most favorable usage, connotes a compulsive programmer who explores, tests, and pushes computers and communications

systems to their limits, often regardless of the consequences. More seriously, it can involve the destruction or sabotage of valuable data, involving massive cost.

According to the security administrator for CompuServe Incorporated, of Columbus, Ohio, the typical hacker is a juvenile with a home computer who uses computerized bulletin board systems (BBSs) for a variety of illegal purposes. Access to such systems requires use of a modem, a device that permits computers to communicate over telephone lines. After buying a modem, the juvenile starts to communicate with others through local BBSs and learns that he can use the BBSs to make friends with people around the country. Since his parents oppose an expensive monthly phone bill, the juvenile must find ways to reduce or eliminate the expense of contacting the distant bulletin boards.

Unfortunately, some board users share stolen telephone access codes (MCI, Sprint, AT&T, among others), and the methods used to determine the codes. The juvenile may use those codes or may try to identify codes himself; computer programs are available to automate the procedure. If he succeeds, he may share or trade codes. Although the juvenile knows these activities are "not quite legal," he thinks he is safe since so many others are involved.

So-called hackers may also become involved in using stolen credit card numbers to arrange mail-order purchases for delivery to vacant homes, where the delivery may be intercepted and kept. Stolen credit card numbers can also provide temporary access to a range of remote computing services, such as those provided by CompuServe Incorporated. Through a fraudulent application, the juvenile becomes a subscriber to the information service, and supplies the stolen credit card number for payment. Although access is temporary (such fraud is not difficult to identify), the juvenile is then involved in activities that include credit card fraud, wire fraud, and various other federal violations, as detailed in the Computer Fraud and Abuse Act of 1986 (Title 18, Section 1030).

Law enforcement officers who handle hacker cases say that some hackers will retaliate if they or their BBS friends are criminally investigated. Retaliation can include destroying the credit histories of the law enforcement officers involved in the investigation or creating enormous bills on their phones or utilities.

Automatic Teller Machine Frauds

Many state computer crime laws specifically or by implication cover frauds involving Automatic Teller Machines (ATMs). Philadelphia is one jurisdiction with considerable experience investigating such cases. Originally, these cases involved persons with legitimate bank accounts who made

fraudulent deposits (e.g., depositing empty envelopes) and then withdrew money from their accounts based on those deposits. Now that banks photograph persons making deposits and withdrawals, the criminals use others to act as intermediaries and make withdrawals. Even with the use of cameras, ATM cases are hard to prove because it is difficult to locate the offenders.

Interestingly, the police are finding that ATM cases do not involve the typical white-collar offender. People arrested for ATM frauds have extensive prior records, including arrests and convictions for violent crimes, which leads investigators to speculate that ATM fraud may be replacing robberies and burglaries for some offenders.

Records Tampering

Although information has always been regarded as valuable (witness the number of civil suits that center on loss or distortion of information), computers have made the storage, alteration and loss of information far more likely than before. Because of the abundance and accessibility of computer records, everyone is vulnerable to having their credibility and finances destroyed by individuals using computers. Many state legislatures as well as the federal government have responded by defining computerized information as valuable property, whose theft, alteration, or destruction is a crime.

Alteration of computerized information can involve issues of the public trust. In a 1985 Colorado case, the former Golden district attorney was prosecuted for having another public official change the district attorney's driving record to remove speeding tickets. The district attorney was charged with computer crime under Colorado's statute, and was tried and convicted. The conviction has since been upheld on appeal.

Unauthorized access to information can be more insidious. The assistant attorney general responsible for prosecuting computer-related crimes in Arizona recounted a case in which a police officer shot at his girlfriend and was charged with attempted murder. While awaiting trial, the officer asked five friends in different police departments to check the names and addresses of all the witnesses to the crime. Presumably the offender intended to intimidate the witnesses to keep them from reporting their observations of the offense. Subsequently, the man killed his girlfriend, and his friends were charged with computer crime for having accessed computerized information without authorization.

Crimes Committed by Disgruntled Employees

Many businesses fall prey to employees who commit an array of computer-related offenses. Large businesses may choose to absorb the losses

rather than face the consequences of public disclosure, but many small businesses do not have that luxury. Experts believe that a small business in which only one or two people are familiar with the computer system has few resources and little resiliency to recover from computer-related losses.[6] Many investigators anticipate that small businesses will need to rely increasingly on the public sector for a solution to computer-related crimes.

A typical offense involving a disgruntled employee occurred in Arizona. On the eve of leaving a small business, an employee changed all of the employee passwords, potentially affecting the production of W-2 tax statements. Later, the former employee demanded a ransom for the altered passwords. Although they did not meet her demands, company executives also did not press charges.

In another case, a detective in the Lakewood, Colorado, police department was contacted by a local sheriff's office after the office's phone system was shut down by a former employee of a major telecommunications company. Shortly after being dismissed by the company, the former employee retaliated by using his knowledge of the computer that channelled calls to shut down the phone systems in all of the company's big accounts. The employee first eliminated the memory in a large airline's phone switching system, making it impossible for employees either to receive or make calls and effectively shut down business for a day at thousands of dollars' expense. He then proceeded to do the same thing to a large petroleum company. When the oil company contacted the phone company, the latter simply said there had been some trouble with the lines, although it appeared subsequently that the phone company was suspicious about the actual cause of the problem. The former employee then proceeded to shut down the phone systems in two banks, a life insurance company, and two municipal governments. In each case, the phone company claimed there was a phone line problem. It was only when the offender terminated service in a local sheriff's office and a workman who was sent to repair the problem admitted that the phone company was having difficulty with a hacker that the series of crimes was detected. The phone company then confessed that they suspected that a disgruntled employee who had been marketing security systems for them before his dismissal was shutting down the systems in the victim organizations. The suspect was ultimately charged with all of the offenses.

Child Pornography and Abuse

In Philadelphia, officers in the city police department's sex crimes unit began monitoring publicly available computer bulletin boards after receiving information that the boards were being used to transmit information on child pornography. With federal grant money, the two adapted a city computer to tie into a legitimate bulletin board. Monitoring of the board led to the arrest

and prosecution of a person seeking child pornography. The suspect, who was seeking to have pornography delivered by U.S. mail, had previously been arrested by the FBI for a similar offense, and was detected simultaneously by an Oklahoma trooper and the Philadelphia officers who were monitoring bulletin boards in their respective locations. Ultimately, the case was prosecuted federally.

Computers may also be used more directly in crimes related to child sexual abuse. Child pornographers in the Philadelphia area are known to send pornographic pictures in computer-to-computer transmissions, and to keep records of criminal transactions in computer files. In Middlesex County, Massachusetts, prosecutors have repeatedly observed the utilization of computers and computer networks by child abusers. Typically, the victims in these cases are young boys between the ages of 9 and 14. The adult offender generally uses his home computer and the electronic bulletin board systems to develop relationships with the boys. At times, in an effort to silence difficult victims, offenders will use computer networks even to transmit threats of physical harm. In some cases, law enforcement officials have also uncovered diary accounts of sexual abuse included among the automated records in an offender's home computer system. In most instances a working knowledge of computers is required in order to investigate the cases properly.

Drug Crimes

A concern expressed repeatedly among those interviewed for this project is that drug offenders are using advances in automation to further their business deals. Earlier in this section it was mentioned that automation in the communications industry has created the possibility for drug dealers to communicate anonymously with each other. It has also been reported that searches of crime scenes involving drug offenders frequently uncover computerized records of drug deals. In a recently reported case, federal agents raided a motel room in Florida, obtaining evidence of a multi-million dollar drug smuggling ring. One piece of confiscated information, a slip of paper listing two names, led to the discovery that the two individuals were IBM employees hired by the ring to help computerize its smuggling operations[7].

Yet in spite of the growing use of computers, the value of computerized records to the investigation of drug crimes is not always recognized, especially by investigators unfamiliar with computer technology. The co-chairperson of Brevard County, Florida's Law Enforcement Technology Assistance Committee (LEETAC) highlighted this point when he described an incident that occurred recently in that County. During a raid on a major narcotics operation in the County, law enforcement officers encountered considerable computer equipment. Unfortunately, the officers were unaware of the potential

significance of the evidence and unfamiliar with computer operations, so the computer equipment was not collected with other, more traditional evidence.

Organized Crime

Of growing concern is the role of computers in furthering the ventures of organized criminals. Reported cases include the use of computers in connection with organized prostitution, pornography, fencing, money laundering and loansharking. Any investigator involved in the investigation of these types of crimes should thus be prepared to collect and analyze computerized evidence.

Indeed, much of what has been reported during the course of the current study involves organizations of offenders. For example, in a typical scheme known as a boiler room operation, criminals organize a fake company. They use a computer to uncover long distance phone codes and make calls to companies and individuals (generally out-of state) offering unusual discounts on products of interest. Using credit cards, the recipients of the calls place orders for the fictitious products. After the boiler room operators process the payments, they close down operations and move on. The victims receive no merchandise. Since the offenders usually call from distant locations, they generally have disappeared before investigators can discover them.

The Special Agent in Charge of the Fraud Division of the U.S. Secret Service described a telecommunications fraud that required the simultaneous delivery of 24 search warrants throughout the United States. Members of the ring approached legitimate businesses offering incredibly low long distance rates. In essence they sold the companies stolen phone codes, but claimed that they were selling unused portions of WATS services sold previously to other companies. Allegedly the unused portions of the services could be recycled to other companies, resulting in half the phone bill the company normally paid. Since the amounts of remaining phone time were variable, the criminals claimed, the length of time that the service could be used by the subsequent company would also vary. Consequently a new code would likely be necessary every few days and the subscriber needed only to call for a new code. Of course the need for a new code was not prompted by the variability in the amount of WATS time that remained, but by the discovery of code abuse by the phone companies, which quickly destroyed the codes.

Endnotes

1. August Bequai, *How to Prevent Computer Crimes: A Guide for Managers* (New York: John Wiley and Sons, 1983): 43.
2. Donn B. Parker, *Computer Crime: Criminal Justice Resource Manual* (Washington, D.C.: National Institute of Justice, 1989): I-3.
3. Donn B. Parker, "How Much Computer Abuse is There?" (Menlo Park, CA: SRI International, 1981): 7.
4. Parker, *supra*, note 1, at I-3.
5. Richard C. Hollinger and Lonn Lanza-Kaduce, "The Process of Criminalization: The Case of Computer Crime Laws," *Criminology*, Vol. 6, No. 1 (1988): 112.
6. See *A Small Business Guide to Computer Security*, prepared for the Computer Security and Education Council, Small Business Administration, April 1987, p.2.
7. August Bequai, *Technocrimes* (Lexington, Massachusetts: Lexington Books, 1987): 65.

Chapter III: Investigation: Current Practices and Procedures

The investigation of computer-related crime entails special challenges not encountered in many traditional investigations. These include:

- Computer-related crimes and their victims often require a proactive enforcement strategy of contacting potential victims and developing investigative capabilities in advance of the reporting of an offense, rather than the reactive approach utilized in most law enforcement agencies.
- For public relations and other reasons, victims of computer-related crimes may hesitate to report their victimization, thus failing to trigger even a reactive law enforcement response.
- Computer-related offenses require a considerable investment of time, but may result in a relatively small number of arrests. Law enforcement agencies that rely on clearance rates as their primary measure of success are hard-pressed to justify expenditures for computer-related investigation.

Recognizing these challenges, it is nonetheless possible to develop strategies to meet them.

Site Studies of Computer-Related Investigations

In a few sites around the country, investigators are developing skills to combat computer-related crimes. Typically, the capability to investigate these crimes has emerged in one of two ways: a few self-starting officers with some computer knowledge have lobbied their agencies to develop expertise in computer-related investigations, or reports by victims of computer-related crime have prompted law enforcement to respond quickly to a new type of offense. The case studies that follow exemplify workable models for the development of investigative strategies.

Maricopa County, Arizona

Maricopa County, Arizona is home to nearly 2 million people, hosts headquarters of GTE-Sprint, Honeywell, INTEL, Motorola, and Sperry, and divides its jurisdiction among 30 law enforcement agencies. Crimes occurring in the unincorporated areas (roughly 88% of the land area) are investigated by the Sheriff's office, which has over 1,700 employees. In addition, the Attorney

General's office and the county attorney's office have staffs that investigate certain crimes. Law enforcement officers are empowered to work anywhere in the state, but generally members of the Sheriff's office only handle unusual cases in the incorporated areas (i.e., those involving organized crime or computer crimes).

The Sheriff's office has a special computer crimes unit, which was created in 1984 when the Sheriff's department established a computerized bulletin board to communicate with the community. Shortly after the board was established, someone posted an offer to modify cable T.V. convertors for $15 so that consumers could receive free cable service. One of the officers monitoring the board investigated and the offender was charged with felony theft of the cable T.V. service.

Although that case did not involve computer crime, the investigator recognized the bulletin board's potential for sharing illegal information. Soon, the bulletin board was involved in the investigation of telecommunications fraud, computer fraud, and credit card fraud. Eventually, a bulletin board was used in a sting operation, which lasted for nearly a year and resulted in several arrests.

In the two years following the creation of the two bulletin boards, the computer crimes unit investigated approximately 80 cases, two-thirds of which were referred to the prosecuting attorney's office. One investigator acted as the personal computer expert and the other as the telecommunications expert. A major portion of the investigations involved telephone hackers, about 90% of whom were juveniles. In addition, the investigators made between 100 and 150 public speeches and wrote several articles for computer journals and magazines.

Lakewood, Colorado

The Lakewood, Colorado, Police Department, established in 1969, has about 200 officers and serves a city of approximately 150,000 people. The city is part of Jefferson County (population nearly 500,000). All of Lakewood's officers are college-educated, which may explain their unusually high level of computer experience. Because the department is relatively new, the force is young: the average officer is 33 years old with eight years' experience. In 1983, the department began purchasing microcomputers with the primary intent of improving the office's word processing capability.

The detective who handles computer-related investigations joined the department in 1972, and has spent the past five years in intelligence, the unit responsible for handling computer-related crimes. In 1981, the detective began using a departmental modem (then rare in police departments) to tie into computerized bulletin boards to gather intelligence. He soon found that considerable illegal information was being shared among some board users.

By 1983, he set up a departmental bulletin board to share law enforcement information and to communicate with youths regarding computer law and ethics. He discovered a number of juveniles and some adults sharing phone codes and credit card numbers.

In 1986, he and other law enforcement officers formed the Colorado Association of Computer Crime Investigators (CACCI) to discuss computer crime, review developments in computer technology, investigate and prosecute computer-related crimes, and develop training programs. The roughly 40 members are given duty time to participate. They include local law enforcement officers, private security consultants, and representatives from the Air Force OSI and the U.S. Secret Service. The Association has had great difficulty attracting prosecutors, however.

Columbus, Ohio

The Columbus Police Department, serving a city of over one half million residents, first became involved in the investigation of computer-related crimes when MCI reported that a hacker had used a personal computer to steal long-distance codes and made hundreds of illegal calls. An officer with his own personal computer investigated the case and, five years later, is the city's sole investigator of computer-related crimes. The Organized Crime Bureau, where he works, reports directly to the Chief of Police, who is interested in computers and computer-related crimes and has been attentive to most of the Bureau's equipment and support needs.

Shortly after his first investigation, that officer and several others in the department were trained in computer crime investigation at the Federal Law Enforcement Training Center in Glynco, Georgia, but only he has pursued his interest.

The need for additional personnel is acute, however; without some restructuring, the department could lose its investment in computer crime investigation. The computer-related crime investigator must spend three-fourths of his time maintaining the bureau's computer system, which is used for word processing, data base management, and as a link to various federal and city justice data banks.

Since embarking on his first investigation, the officer estimates that he has investigated 15 computer-related crimes (at least half involving joint ventures with other departments) and charged seven individuals, all resulting in convictions through guilty pleas. All but three of the cases have involved juvenile "hackers." One involved a disgruntled employee who copied from the computer system most of the company's proprietary information before he left the company.

Philadelphia, Pennsylvania

On January 4, 1988, the Philadelphia Police Department formed a seven-person economic crime unit, the outgrowth of several investigations (many of them computer-related). Two people were instrumental in the development of the unit: a detective who specializes in computer-related crimes and the city's former Commissioner of Police, who once headed a Secret Service fraud commission and knew the importance of economic crime investigation.

The detective with primary responsibility for investigating computer-related crimes began handling those crimes in 1983. A 19-year veteran of the force, he has experience as a detective in an investigations unit specializing in high visibility crimes, i.e., armored car robberies, bank robberies, and kidnappings.

While working in special investigations, he first met an assistant district attorney who handled computer-related prosecution. He also was approached by a bank manager concerned about an embezzlement involving the bank's computer. As the detective investigated the case, he was directed to the District Attorney's economic crimes unit and its specialist in computer-related frauds. The detective continued to bring computer-related frauds to the assistant prosecutor from 1983 to 1986, and began developing an economic crime section in the police department.

He now has a partner, who formerly worked the general crimes desk. Neither detective has had any formal training in the investigation of computer-related offenses. In fact, the only training either received was from the former assistant district attorney, who instructed them on the preparation of computer-related search warrants.

Before the creation of the Economic Crime Unit, most of the roughly twelve cases per year that the detective presented to the District Attorney's office involved ATM frauds. During the first eight months the Economic Crime Unit existed, the two detectives handling computer-related cases estimate they made over 50 arrests, about half of them for computer-related crimes. A majority were ATM cases. Monitoring of bulletin boards and activities involving electronic surveillance have not occurred, largely because the economic crimes section does not have its own computers or modem, and Pennsylvania law makes it difficult for law enforcement officers to conduct wire taps. Consequently, the department rarely investigates the kinds of telecommunications and hacker cases reported by other jurisdictions.

The Nature of Computer-Related Investigations

Although approaches to investigating computer-related crimes vary, the nature of the work is similar in most respects. First, investigation of computer-

related crime requires a considerable investment of time. Depending on the type of case, estimates for a thorough investigation range from four months to one year. In cases involving the use of communications systems and bulletin boards, considerable time must be spent on electronic surveillance. Because criminals in those cases use computers to communicate quickly among themselves, and because search warrants in computer-related cases are complicated, a considerable amount of investigative work must occur before warrants are issued. In situations where surveillance may not be required because the crime occurred in the past (e.g., in embezzlements), investigation of computer-related crimes often requires reviewing large quantities of computer data for evidence. Investigating an 18-year-old who had defrauded area investors out of $1,000,000, a criminalist with the Jefferson County, Colorado, Sheriff's Department analyzed over 80 computer diskettes and produced 11 notebooks of evidence.

Second, investigation of computer-related crimes involves interaction with victims. Often victims familiar with their own computer systems are asked to assist investigators. When businesses are victimized, investigators must at least use the victims to determine the role that the computer plays in the organization and to identify the persons who have access to the computer system. Victims may provide considerable technical support as well.

Third, the work has been described as largely investigative by those who do it. One police officer noted that it is 90% traditional police work and 10% technical skill. In a recent paper, Secret Service Agent Stephen Purdy, who has dedicated the past three years to computer-related crime investigations, outlined the following similarities and one major difference between the investigation of computer-related crime and investigations of more traditional crimes.

> Investigating computer crime employs many conventional techniques. Physical evidence still needs to be identified and collected. In computer fraud, physical evidence may take the form of sales invoices, computer printouts, handwritten notes, photospreads, fingerprints, computer audit trails, telephone toll records, pen register records, wire intercept transcripts, etc. Conventional investigative techniques such as surveillances, use of informants, witness and suspect interviews still apply. Circumstantial evidence is also found in computer crime investigations. In fact, there are very few differences between computer fraud and any other type of fraud, except the device used to commit the fraud—*the computer.*[1]

Finally, the very private nature of computer-related crime often necessitates a proactive approach to its investigation. Whether it is monitoring computer bulletin boards or speaking routinely to local schools and businesses, most investigators agree that there is both need for proactive

investigation of computer-related crime and return for the effort in increased prevention, detection, and reporting of crimes.

Handling the Investigation

The unique challenge of computer-related crime investigation is understanding computer operations well enough to obtain necessary information and evidence from the computer, either personally or with expert assistance. In many ways a computer is nothing more than a file cabinet, but one requiring training and expertise to use.

Provided that the circumstances of the case make it feasible, there are a number of reasons why it is desirable for investigators to conduct a thorough investigation before executing a search of the scene of a computer-related crime. First, the more that is known about the type of activity in which a criminal is engaging, the type of computer equipment being used, the number of persons involved in the crime, the amount and kind of peripheral equipment (e.g., computer modems, telephones, printers) present, and the kind of paper records that are being kept, the more specific the warrant can be. Second, investigators can avoid many delays if they know in advance what to expect at the crime scene. Delays can be especially costly if speedy trial laws are applied stringently in an area. In some instances, such as those involving computerized telemarketing schemes, confiscation of evidence generally requires confiscation of the entire computer system, which can be tantamount to closing down the business. Delays in those instances can be quite costly: when the business has not already been established as illegal, closing it down by confiscating evidence can result in liability suits or in a judge's terminating the investigation. Additionally, knowing about the crime scene in advance can help to determine whether there is a need for experts to be present when collecting evidence.

It is not unusual for investigators to consult experts from other investigative agencies, local universities, or the private sector when conducting a search of a crime scene. Comprehensive knowledge of all new technology is virtually impossible even for those dedicated to such tasks. Some critical mistakes in evidence collection and analysis can be avoided if there is advance warning about what the investigator is likely to find at the crime scene. Finally, knowing as much as possible about the intricacies of the case can help prevent some unfortunate mishaps. For instance, it is important to know when to conduct a search. As stated earlier, many computer-related cases involve networks. It is very easy to lose co-defendants and evidence unless there is careful planning, because persons communicating by computer can quickly alert each other that others in the organization have been arrested. The Secret Service case involving communications fraud, for example, required careful planning to assure

the simultaneous delivery of 24 search warrants in locations ranging from Florida to Hawaii. When personal computers are used in a crime, the attempt to execute a search during the commission of a crime may lead to the criminal's destroying evidence before or during the service of the warrant.

Accomplishing thorough investigations in computer-related cases increasingly means relying on surveillance of the crime scene, use of informants, undercover operations, and a host of electronic devices. The most frequently mentioned piece of equipment is a pen register or dialed number recorder (DNR), as criminals frequently use the phone lines in the commission of computer-related crimes. The Secret Service lists the following guidelines in preparing for the search of a crime scene in a computer-related case involving personal computers.

> Learn as much about the occupants of the crime scene as possible, including the number of residents and their employment and educational backgrounds. The intent is to establish the occupants who could commit the crime. If only one resident knows anything about computers the likelihood of any other resident's committing the computer crime is reduced.
>
> Review the telephone records of all phone lines to the crime scene.
>
> Explore the possibility of developing an informant.
>
> Observe the habits of the suspect.
>
> If phone abuse is involved, use a DNR to collect evidence. Note that DNR records will not be sufficient evidence of the suspect's involvement in the crime if anyone other than the suspect could have committed the crime.[2]

In a computer-related case an affidavit for a warrant should be very detailed, including descriptions of phone records and other information collected during the investigation. Samples of an affidavit and search warrant for a case involving telecommunications fraud are included in Appendices A and B. Investigators who work regularly with one prosecutor suggest that a prosecutor be involved when application for a search warrant is made to discuss in advance the evidence necessary for prosecution and evidence collection strategies.

The Crime Scene: Collecting Evidence

As with any criminal case, careful collection of evidence is critical to successful prosecution. Investigators may need to bring equipment to the crime scene that may not be available during a standard search, and must collect evidence without losing or changing originals. Recent literature, summarized

below, describes the equipment and evidence collection issues involved in searches of personal computers.[3]

Computers are unique as sources of evidence in several ways:

- Computers use electricity. Any interruption in the power during data manipulation could result in the loss of important information.
- Computers are sensitive to disruption by moving, even when turned off. If there is a hard disk drive, the heads on the drive should be "parked" before moving the system to avoid destroying stored information.
- Magnetic storage media, such as removable diskettes, are vulnerable to damage by exposure to magnetic fields that can be produced by such things as stereo speakers and printers.
- Many additional pieces of equipment, such as telephone modems, auto-dialers (programmable telephones), and printers, may be connected to computers. It is important to document how the system is organized and to know when and how to disconnect those pieces of equipment from the system. Otherwise, important information can be lost.
- Before disconnecting an auto-dialer, it is important to ascertain what it contains. By attaching a DNR to the auto-dialer, the crime scene investigator can obtain a printed record of the phone numbers and access codes stored in the dialer's memory.[4]
- Because computers are intended for the storage of information, investigators must be careful not to change data while collecting evidence. Specifically, this means that all portable disks should be protected so that they may not be written on.
- When analyzing evidence, investigators must work with copies rather than originals. This protects against inadvertent changes to the content of the originals, as well as defense arguments that the originals have been altered.

Investigators may not always know in advance that computer equipment is present at a crime scene. Narcotics investigators, for instance, may be surprised to find an array of computers, printers, printouts, and other computer materials during a crime scene search. A standard procedure should therefore be established for collecting computer evidence in situations in which its collection was not anticipated and in which crime scene investigators have not been trained in the collection of computer-related evidence.

Evaluating Evidence with Expert Assistance

Review of the information stored in a micro computer system can require knowledge of the computer's operating system and file structure, as well as an array of basic programming languages, such as d-BASE III, Lotus 1-2-3, and word processing languages. Investigators have also found that they can collect considerable paper, including hand-written notes, printouts, and manuals, at computer-related crime scenes. These materials, once evaluated, can reveal important information about the computerized evidence.

In situations involving large mainframe computers, additional concerns about protecting and analyzing the data arise. A mainframe computer cannot easily be isolated from the crime scene in order to protect the information. It may be unclear who is involved in the crime, but undesirable to disrupt the access and activities of legitimate users. Moreover, operating systems and programming languages are different in a mainframe context than in one involving personal computers.

Even the best trained investigator cannot know everything about each computer system, all pieces of peripheral equipment, and every programming language that could be encountered during a crime scene search. Hence most investigators have quickly realized that they must rely on a range of experts to assist with investigations.

Relying on the Victim

At some point almost every investigator has relied on victims as experts; many swear by it. But using victims in this way does raise several concerns. One is that the investigator requires the victim to make a financial commitment in excess of the loss from the computer-related crime. Another is that in some instances it is not clear who has committed the offense. The person apparently in the best position to assist the investigation may also be a prime suspect.

Utilizing Talented Agency Personnel

Most jurisdictions have expanded their lists of experts. One of the best strategies is to locate persons within the agency or related agencies who have computer expertise. This may mean receiving technical support from persons outside the unit directly handling the investigation. In Jefferson County, Colorado, the Sheriff's office recruits the talents of their in-house criminalist whose primary job is the chemical analysis of evidence. Another option is to employ reserve officers with computer skills. In some sites, reserve officers are on-call to provide technical assistance in the collection, evaluation, and presentation of computer-related evidence.

Finding Support in the Private Sector

Other possibilities include establishing contacts with local schools and businesses to identify advisors who can support computer-related investigations. In this regard the Information Systems Security Association (see Appendix C), which has chapters in many states, has proved a useful resource for locating computer experts in the private sector. University professors and graduate students have also been helpful.

In several locations, investigators have combined the talents of public and private sector experts and developed innovative strategies for investigating computer-related crimes. The police department in Lakewood, Colorado, forms a special computer crime team as soon as a computer-related crime is detected. The team consists of a technical coordinator from intelligence, a fraud investigator, a senior coordinator (the Sergeant in charge of intelligence or the Sergeant in charge of fraud), others in the department (e.g., a patrol officer with key punch experience), and others in the local community (such as representatives of the victim organization), as necessary.

Sharing Resources

Agencies with technical experts have also established procedures for sharing their expertise with other, often smaller, agencies. When a crime occurs outside of Lakewood, Colorado, representatives from Lakewood may be loaned to the investigating agency and Lakewood pays the loanee's salary. Almost all of the law enforcement agencies in Colorado, and especially in the Denver area, work cooperatively, and often share officers with particular talents. Generally, these arrangements are made among investigators and are communicated to the sergeants in charge. Chiefs and Sheriffs are not necessarily involved.

Federal, state, and county associations (e.g., the Federal Computer Investigations Committee, the Colorado Association of Computer Crime Investigators, and the Law Enforcement Electronic Technology Assistance Committee in Brevard County, Florida) also facilitate the sharing of knowledge about computer-related crime investigation and prosecution. These groups share the same general goals: providing technical training to members, sharing intelligence about computer-related cases, and sharing technical expertise. Associations afford access to a broad base of technical knowledge, allowing each member to serve as the primary computer expert in the agency he or she represents. Finally, through their voting membership and roster of guest participants, the associations build a bank of community experts who can be contacted when complex computer issues arise.

The Colorado Association of Computer Crime Investigators meets roughly every two months and provides a newsletter to the membership between meetings. Only a portion of the members have strong technical

backgrounds. Some members from small law enforcement agencies participate because they do not have the resources to have experts on their staffs, but still need to maintain contact with investigators who do have the skills necessary to investigate computer-related crimes. Most of them have not actually encountered any computer-related offenses as yet, but would contact association members to establish a task force of experts if a crime was reported to them.

In Brevard County, Florida, prosecutors from the State's Attorney's office and investigators from ten of the County's 16 law enforcement agencies have formed the Law Enforcement Electronic Technology Assistance Committee (LEETAC), which operates a 24-hour computer hotline for investigators in need of technical assistance with computer-related cases. Typically, LEETAC members are involved in a computer-related case when a local investigator contacts his or her agency's LEETAC representative for assistance. That representative and others from the association then facilitate the handling of the technical aspects of the computer-related case.

Although the Committee is only a few months old, members have already assisted in the preparation of computer-related search warrants, the use of dialed number recorders (DNRs), and the development of a base-level training program for all law enforcement officers in the County. Currently the Committee is developing a training videotape that will be available to each law enforcement agency in the County.

More information on these and other associations is provided in Appendix C.

Endnotes

1. Stephen R. Purdy, *Computer Crime Investigations*, Draft Monograph, Federal Computer Investigations Committee, 1988, pp.2-3.
2. Purdy, *supra*, note 1, at 6-10.
3. James Conser, Louis P. Carsone, and Robert Snyder, "Investigating Computer-Related Crimes Involving Small Computer Systems," in *Critical Issues in Criminal Investigations*, 2d ed., Michael Palmiotto, ed. (Cincinnati, Ohio: Anderson Publishing Company, 1988): 35-58; and Purdy, *supra*, note 1 at 10-18.
4. Purdy, *supra*, note 1, at 15.

Chapter IV: Prosecution: Current Practices and Procedures

Just as there are few law enforcement officers who specialize in investigating computer-related crime, it is not typical for prosecutors to have expertise in computer-related prosecutions. One reason may be that until recently only a handful of law schools offered any courses on the subject. Although still not large, the number of schools including some coursework in computer law is growing. (See Appendix D for more information.) Additionally, many prosecutors' offices have not yet recognized that computer-related prosecution is a unique activity. Some of this probably results from the fact that there are few investigators handling computer-related crimes and very few victims willing to report them. Consequently most prosecutors have not been presented with a large volume of computer-related offenses. Even when a case involving computer evidence is presented, the tendency for prosecutors to avoid charging a computer crime may also serve to dilute the apparent need for specialized prosecution skills. Computer-related crimes may be handled simply as white-collar crime, traditionally a low priority in many prosecutors' offices. Finally, many prosecutors' offices do not have even basic computer equipment, and thus do not encourage the development and use of computer skills.

Those who prosecute computer-related cases have demonstrated a real interest in the subject and have sought out the cases. Often they have learned by trial and error what makes computer-related prosecutions difficult and unique. Rather than being intimidated by the difficulties associated with computerized evidence, they have concentrated relentlessly on developing an understanding of those cases.

Site Studies of Computer-Related Prosecutions

The following descriptions of prosecution efforts in several sites will demonstrate how the ability to conduct computer-related prosecutions has evolved.

Maricopa County, Arizona

Although computer-related crimes in Maricopa County are prosecuted by the County Attorney's office, they may also be prosecuted by the State's Attorney General's office. The office has jurisdiction over white-collar crimes and cases involving organized crime. Computer fraud is a racketeering offense in Arizona. Since many computer-related crimes involve networks of people,

they are suitable for prosecution as organized crimes; but it is only by an informal arrangement that many computer crimes are now being processed by Arizona's Attorney General's office. The unwritten understanding among state and local law enforcement officials is that cases will be brought by local law enforcement to the Attorney General's office if the primary offense is a computer crime, but taken to the County Attorney if the cases involve a number of offenses in which the computer crime is perceived to play a minor role.

The Attorney General's office has taken a leading role in part due to their recruitment in 1981 of an assistant attorney general who specializes in computer crime prosecution. At that time, detectives in the computer crimes unit in the Maricopa County Sheriff's office had begun to generate a large number of cases. At first the new computer specialist in the Attorney General's office received only the cases that the county attorney rejected, but in a short while cases were referred by other agencies. Now many cases are initiated directly with the Attorney General's office, some coming from the Sheriff's office and others reported directly to the Attorney General's office specialist by contacts in the business community familiar with her work. The Attorney General's office also has an investigator to investigate computer-related cases brought directly to them.

The assistant attorney general estimates that she has about 15 to 20 investigations open at any one time, most of which are highly complex.

Columbus, Ohio

As soon as the Columbus Police Department discovers a computer-related crime, either by being alerted by the victims or by monitoring bulletin boards, the officer responsible for investigating those crimes goes to the Franklin County Prosecuting Attorney's office. Over the years, he has developed a close working relationship with the prosecutors in the economic crime section of the prosecutor's office. Although most cases involve juveniles and result in guilty pleas, those prosecutors assist with warrant preparation, charging decisions, and the preparation of indictments.

The officer in charge believes the investigation of computer-related crimes requires a strong relationship between the investigator and the prosecutor, which ideally translates into vertical prosecution from screening on. Part of the reason for this is that he feels he can work swiftly with a prosecutor who has been trained in the technicalities of investigating computer-related crimes.

In Franklin County it is possible for an investigator to bring a case directly to the attorney of his choice and bypass the screeners in the office's grand jury-intake section. It is also common for investigators to seek direct indictments of felons, rather than making arrests and filing them in the

municipal court where they filter slowly through prosecutor screening and municipal court bind over proceedings. Such a structure facilitates the building of close working relationships among prosecutors and investigators. Moreover, the complicated nature of many of the cases that have been investigated in Columbus to date often demands that indictments are prepared in secret to avoid having suspects destroy evidence before arrests are made.

Both prosecutors in the economic crime section were trained in computer crime prosecution at the U.S. Treasury Department's Federal Law Enforcement Training Center in Glynco, Georgia. However, their training came after they had been working several years and may have been too basic. Since there is very little money for training, it is considered an incentive that only senior attorneys receive.

Denver, Colorado

For a number of years the prosecution of computer-related offenses in Denver was the responsibility of an assistant district attorney who co-authored Colorado's computer crime statute and prosecuted 12 computer-related crimes during his tenure. Shortly after joining the staff of the Denver City District Attorney's office in 1972 (even before there was a computer crime statute), that assistant and other new attorneys were encouraged to learn about crimes of the future. He volunteered to tackle computer crime and attended a course entitled Computer Crime and Prosecution. The course taught him a way of thinking about the problem, but did not make him a computer expert.

Following his training, the assistant district attorney outlined procedures to assure that computer-related cases were referred to him and that co-workers collected appropriate evidence. First, he made sure that screening deputies sent all cases involving computers directly to him in the complex prosecutions unit. Then he trained the investigators who worked with him not to be alienated because a case involved a computer, and outlined a procedure for collecting evidence. Most importantly, he learned how victim businesses worked. In all of the cases he handled, he relied on the victim to provide the technical expertise; consequently, he did not see a need to have technical people on staff.

His cases fell into two categories: standard thefts involving computers or manipulation of computer data. Six of the 12 cases were filed with computer crime charges; six were filed as thefts. All 12 cases involved adults. The former assistant district attorney feels that the use of computers in the offenses was important, regardless of how the cases were charged, but that the major difference between the two types of offenses was the amount of evidence that would have been introduced if the cases had gone to trial. Prosecutors, he says, should use their discretion to determine how best to get the most out of their charging, though cases involving computers will likely require mention of the computers if they end up in court.

Philadelphia, Pennsylvania

The Philadelphia District Attorney's office employs approximately 215 attorneys. The Economic Crimes section, which is comprised of a chief, two assistant chiefs, and 15 attorneys, handles most computer-related crimes. Attorneys in the private frauds section are assisted by four accountants, ten detectives, one paralegal, and two secretaries.

Interest in computer-related crimes has existed in the Philadelphia District Attorney's office for nearly a decade. A forensic accountant in the Economic Crime unit, who started working there in 1980, is a self-taught expert in micro- and mini-computers who now handles all of the district attorney's office's computer-related investigations and provides technical assistance to the police department. When he needs assistance, he generally turns to experts in the victim companies for understanding of the esoteric aspects of their hardware and software.

In 1981, the office employed an assistant district attorney with a strong interest in computer-related prosecutions. While a part of the district attorney's staff, she was assisted by investigators in the district attorney's office and also worked on many cases brought to her by the Philadelphia Police Department and other law enforcement agencies.

Since that assistant departed to join the staff of the Arizona Attorney General's office, the Philadelphia District Attorney's office has not had a prosecutor with special knowledge of computer-related cases. Although the new chief of Economic Crimes considers that the prosecution of computer-related crimes requires special skills and attention, he does not consider that it requires more skill than prosecutors in the office already possess. Hence, he sees no need to recruit a computer expert.

The Nature of Computer-Related Prosecutions

Prosecution of computer-related offenses is similar in many ways to the prosecution of economic crimes. Both usually require an attention to the details of business operations, patient inspection of copious amounts of evidence, and an understanding of accounting and financial principles. Each requires considerable time for case preparation, resulting in the generation of large amounts of paper. Both appear more likely to result in guilty pleas than trials, although some investigators and prosecutors suggest that computer-related crimes may have a higher incidence of plea dispositions as a result of the reluctance of both defense counsel and prosecutors to introduce complicated computer evidence in court.

The prosecutor who tackles computer-related crimes must also understand how computers operate, how they are used by victims, and the

similarities and differences between computer-related evidence and evidence used in other types of cases. He or she must know how to present computer-related evidence so that it not only meets all evidentiary requirements, but also is comprehensible to a judge and jury. This requires sufficient technical understanding to communicate with experts and use them as witnesses effectively. Because many investigators lack specialized training for collecting computerized evidence, prosecutors of computer-related crimes may need to know more about the collection of the evidence in computer-related cases than in other types of cases. In successful prosecutions of computer-related crimes, partnerships between investigators and prosecutors are formed early in the investigations.

Computer-Related Evidence

The key to prosecuting computer-related crimes is understanding computer-related evidence: knowing how it is collected, what its strengths and weaknesses are, and how it is best presented in court. Computerized evidence is documentary in nature, therefore requiring consideration under the best evidence and hearsay rules. Also, establishing a proper foundation to show that the evidence is relevant, accurate, and reliable may be difficult. Commentators note, for instance, that it is probably easier to establish the reliability of documents from a doctor's office than from a gambling operation.[1] Finally, computers are still very unfamiliar to many judges, juries, and attorneys, which forces prosecutors to present information on input, storage, and output of computerized data without excessive computer jargon.

There are several technical accounts of the litigation issues associated with computer-related evidence.[2] What follows here is a summary of concerns raised.

First, in order to lay an adequate foundation in a computer-related case, the prosecutor must authenticate the evidence. Although authentication is fundamentally the same in all types of cases, in computer-related cases it involves providing a satisfactory explanation of the method for collecting information, the process of inputting and storing information in the computer system, the method for retrieving information, the procedure for protecting computer records from unauthorized access/alteration, and the way the organization relies on the computer records in its daily business.[3] The prosecutor must show the reliability and accuracy of all source data entered and recorded in a computer system. He or she must provide a description of any diagnostic tests used to check for defects in the equipment and programs. The prosecutor must also describe the operation and accuracy of the hardware and software, and must show that what is printed is an accurate reflection of what is stored in the computer. All of this verification can involve the use of experts.

Second, all computer-related evidence (if submitted to show the truth of the matter asserted), is hearsay, because it is an electronic representation of a third-party defendant's statements (that is, the operator who entered the data). In order to be admissable, it must fall within the scope of exceptions to the hearsay rule. The most commonly used exception in computer-related cases pertains to business records. Since computer output is frequently a form of business records, it may be admissible under this exception. There may, however, be additional concerns regarding the fact that what is represented in a printout is not necessarily an exact representation of what is stored in the computer (e.g., the printout converts data entries into tables), that the printout was not relied on during the regular course of business, or that the printout is not a reliable account of what is in the computer.[4] Other exceptions to the hearsay rule that may be applicable in computer-related cases include those pertaining to former testimony, official records, and admissions by a party in recorded form. In cases in which the collection, maintenance, and retrieval of data are completely automatic, as in situations involving self-generating telephone toll records, it may also be possible to convince the court that the hearsay rule is entirely inapplicable.[5]

Third, the best evidence rule requires that the original of a written document be offered as evidence to prove that the copy is the best representation of the original. Federal Rule of Evidence 1001 defines an original as any output that is readable by sight if proved an accurate reflection of computer stored data. Also, under the voluminous records exception to the best evidence rule, computer records can constitute a summary of a large amount of data; but admissability is left to the trial court's discretion.[6] Because many legal and illegal operations destroy their originals, it can be asserted that the computer printout is the best practical evidence available.[7] Finally, it is also possible to argue that original data are unavailable if they are stored on magnetic media.

Key Decision Points

Early crucial decisions must be made in a computer-related case during the preparation of the search warrant. Because search warrants must be fairly specific, it is necessary for prosecutors to discuss a host of technical issues with investigators, usually requiring both parties to have some understanding of basic computer terminology and use. Participation in warrant preparation can help to assure that all evidence required for successful prosecution is included in the warrant. (Sample search warrant language for several types of problems is included in Appendix B.) In addition prosecutors and investigators can discuss the technical requirements for searches of crime scenes involving computer evidence to ensure that adequate precautions are taken to protect the integrity of the evidence.

An assistant district attorney in Middlesex County, Massachusetts notes another advantage of close working relations between prosecutors and investigators:

> The relative anonymity or confidentiality afforded a criminal by his use of the computer often presents the investigator with only one option: to induce the criminal to act in a way that will produce proof beyond a reasonable doubt of his identity. For this investigative technique to work effectively, both the investigator and the prosecutor must be working together.[8]

After reviewing the evidence, prosecutors must decide whether to charge a statutorily defined computer crime or a more traditional offense such as theft. Often, even in sites in which prosecutors have handled several computer-related cases, the prosecutor chooses to charge a more general offense, such as theft, instead of the computer crime. These prosecutors recognize that although any crime involving a computer may require some discussion of the computer in proof of the case, a computer crime charge will emphasize the use of computer-based evidence, leading to the evidentiary difficulties noted above. Many prosecutors do not feel confident enough with the issues to prosecute under the computer crime statute. Also in some instances, prosecutors believe that little can be gained from the computer crime charge. In some states, computer crimes are misdemeanors, while applicable theft statutes are felonies. In some, sentencing practices suggest that despite considerable effort to prove a computer crime, the resultant sentence is likely to be the same as if only a traditional theft crime had been charged.

The tendency to avoid charging computer crimes meets with mixed reactions from investigators, however. Some feel that a computer crime charge most accurately reflects the nature of the offense and the effort that has been made to investigate the case. Since administrators in law enforcement and prosecutors' agencies do not always recognize that the ability to investigate and prosecute computer-related cases requires special skill, having cases charged as computer crimes emphasizes the specialized nature of the work. Perhaps more importantly, investigators are concerned that by not charging computer crimes prosecutors fail to test the validity of the statutes in court. Without trials, it is impossible to establish case law and difficult to establish investigators as expert witnesses.

As suggested in the evidence section above, if a computer crime is charged prosecutors must prepare for trial carefully. Introduction of computer evidence will most certainly mean that prosecutors must locate and interview a number of expert witnesses. As one commentator observes:

> In order to lay the foundation for a single bank record, it might be necessary to call the bank's custodian of records to

describe how transaction information is collected, a supervisor from the automated banking section to explain the system, a programmer or operations expert to establish accuracy and security, and as many as a half-dozen others to answer technical questions about the hardware, software, or organizational routine as it relates to the creation and maintenance of computer-related records.[9]

Finally, even though most investigators and prosecutors estimate that 99% of the computer-related crimes that have been processed have resulted in guilty pleas, trials and appeals are likely to increase as justice personnel become better versed in the issues associated with those crimes. Consequently, prosecutors are likely to be required to focus increasingly on appeals issues.

The Effect of Case Processing Structure

Prosecutors' offices are often structured so that criminal cases are prosecuted horizontally—one set of attorneys screens cases, another is involved through the point of bindover or indictment, another set is responsible for trials, and still another may be responsible for sentencing proceedings. Although less common, vertical prosecution, in which cases are assigned to one attorney from screening forward, also occurs.

Given the technical nature of computer-related prosecution, the most successful strategy for investigating and prosecuting the crimes involves early and continuing commitment to the case by the prosecutor in the office who is most knowledgeable about computer-related prosecution. Generally that translates into vertical prosecution of computer-related crime, although it has been possible to adjust horizontal processing to accommodate the unique concerns raised by computer-related crimes.

In Baltimore County, Maryland and Columbus, Ohio, computer crime investigators have developed exclusive working relationships with an individual prosecutor who specializes in computer-related cases. In both sites criminal cases may proceed to a superior court following either preliminary hearing proceedings or indictment. The latter course is generally preferable in computer-related cases given the need for speed, and sometimes even secrecy; obtaining indictments also makes it easy to by-pass the lower court screening units in the prosecutor's office and seek the prosecutor with the most knowledge about the case. The one-to-one relationship between investigators and prosecutors has the added advantage of giving one prosecutor considerable experience in handling the computer-related cases in an office.

It is possible to make a strictly horizontal structure work, however. In Philadelphia cases are always screened by the district attorney's charging unit. The most serious economic crimes are forwarded to attorneys in the economic

crimes section. Less serious crimes are retained for prosecution at the municipal court level. Although this system assures that most serious computer-related cases are prosecuted vertically following screening, some less serious ones are prosecuted horizontally.

The former assistant Philadelphia district attorney overcame some of the limitations of this structure by becoming a resource for other prosecutors in computer-related cases, conducting training sessions for other units, and assuring that she would be contacted by screening prosecutors whenever a computer was involved in the crime. Funnelling cases to an office expert could prove critical in detecting serious computer-related crimes that would not normally be forwarded to an economic crimes unit (e.g., narcotics cases that involve computers) and in assisting with the computer-related aspects of economic crimes whose magnitude does not warrant forwarding to a specialized unit.

Regardless of the structure for prosecuting criminal offenses, prosecutors' offices are likely at best to have only a handful of attorneys with the interest and skills to handle computer-related crimes. Procedures should be established so that a prosecutor experienced in computer-related cases either prosecutes all of those cases or acts as a consultant on the computer-related aspects of some cases and as the chief prosecutor in others. To maintain effectiveness, prosecutors' offices must identify staff members with an interest in computer-related prosecutions and assure that those individuals receive support to conduct the lengthy investigations that are required in those cases. In part that support must translate into good pay and maintenance of the function despite changes in administration.

Endnotes

1. James Conser and Louis Carsone, "Computer-Related Crime and Its Investigation," Chapter 2 in *Microcomputers in Criminal Justice: Current Issues and Applications* (Cincinnati, Ohio: Anderson Publishing Company, 1987): 29.
2. Stanley S. Arkin, et al., *Prevention and Prosecution of Computer and High Technology Crime* (New York: Matthew Bender and Co., Inc., 1988): 8-48-8-90; Gail Thackeray, "Problems of Computer Evidence," *The Practical Prosecutor*, National College of District Attorneys, Vol. 1985, No. 2 (1985): 10-11.
3. See for examples *King v. State ex rel., 222 So2d 393, 398 (Miss.);* Capital Marine Supply Corp. v. Roland Thomas, II, 719 F2d 104, 106 (5th Cir. 1983).
4. Arkin, et al., *supra*, note 2, at 8-62-8-67.
5. Thackeray, *supra*, note 2, at 11.
6. Arkin, et al., *supra*, note 2, at 8-61.
7. Thackeray, *supra*, note 2, at 11.
8. Communicated by Assistant District Attorney, Edward Rapacki, in a letter to the author.
9. Thackeray, *supra*, note 2, at 10.

Chapter V: Issues Affecting Investigation and Prosecution

The investigation and prosecution of computer-related crimes may entail many complexities. The inability of statutes to address adequately the range of computer-related offenses, the multi-jurisdictional nature of many computer-related offenses, the reluctance of many victims to report the crime, the need for experts at low cost, the demand for constant training in order to keep up with changing technology, and the need to recruit and retain skilled investigators and prosecutors are among the many challenges that will face justice agencies in the next decade. The following discussion will focus on each of these and describe ways that jurisdictions now doing the job have addressed and continue to address these concerns.

Adequacy of State Laws

To date, 48 states have enacted legislation regarding computer-related crimes.[1] (See Appendix E for a listing of federal and state statutes.) Clearly, a well-defined statute is crucial to the successful investigation and prosecution of computer-related cases. Yet in many states significant refinements are needed. For instance, Massachusetts state laws are inadequate to allow prosecution of juvenile hackers, who comprise the largest group of known computer-related criminals in the state. Perhaps more disturbing, Massachusetts law does not classify property as stolen unless a victim has been deprived permanently of the property. In many computer-related cases this view of theft is unworkable: an employee can steal copies of proprietary information and devastate a company, even though original materials remain stored in the memory of the company's computer system. This type of crime is likely to become an increasing problem for small and large businesses alike.

Considerable attention has been given to examining the problem of the theft of intangible property, as it has been termed, and the issue has served as the centerpiece of several court cases.[2] Although the protection of computer hardware is covered by traditional criminal statutes of larceny, burglary, or vandalism, the intangible nature of computer software makes it more difficult to apply traditional theories of criminal property law, in particular when trying to assess "value."[3] In addition, traditional definitions of theft do not capture the fact that the loss in many computer-related cases is not an instance of dispossession, but rather a case of deprivation of value.[4]

Another problem associated with computer-related statutes involves the issue of intent. This raises the question of whether the "mere unauthorized

access or electronic 'browsing' in another user's computer files constitutes trespassing, theft, or some other form of criminal activity."[5] Consequently most jurisdictions have realized the need to address nonmalicious illegal access, typically treating it as a misdemeanor.[6]

Those interviewed for this project raised additional concerns regarding computer crime statutes. Most investigators and prosecutors contend that the best statutes are those that are general enough to allow for rapid technological changes in the computer industry, thereby requiring minimal amendment. Each of the sites visited for this project seems to have met that challenge, although their approaches to legislation have differed. Colorado, Pennsylvania, and Arizona have enacted separate computer crime statutes. Ohio has responded to the problem by applying a broad definition of computer-related crime to many of its existing statutes. Also, investigators and prosecutors believe that in order to be effective, the penalties for computer-related crimes must be severe enough to serve as a deterrent. One criterion used by victims to determine whether to report locally or federally is the relative severity of the state and federal statutes. Finally, almost all would agree that it is important for statutes pertaining to asset seizure and forfeiture to include the seizure and forfeiture of computer equipment. Many see seizure as a very real deterrent to future crime: without access to their personal computers and modems, for instance, juvenile hackers are rendered helpless. Some victims have even sought computer equipment as partial restitution for losses incurred from computer-related crime.

Multi-Jurisdictional Cases

Computer-related offenses are often interstate in nature, and involve investigators and prosecutors in several local jurisdictions and the federal government. Nearly all crimes involving telephone code abuse are interstate, as are some automatic teller networks. A disgruntled employee who leaves his job and moves to another state may gain access to his former employer's computer system by phone transmissions and trigger a destructive program.

Although there are several federal statutes under which computer-related crime may be prosecuted (e.g., Title 18, Sections 1343, 1362, 1367, 2512, and 2701), two have been used increasingly for prosecuting computer-related offenses: Title 18, Section 1029, concerning fraud and related activity in connection with access devices, and Title 18, Section 1030, the Computer Fraud and Abuse Act of 1986.[7] The United States Secret Service and the Federal Bureau of Investigation are charged with the investigation of crimes that fall under these federal statutes, although the Service handles most cases covered by Section 1029. Of course, given the range of computer-related crimes, other federal investigative agencies, such as the Postal Inspectors and the Drug Enforcement Administration, also investigate crimes involving computers.

Regarding Title 18, Section 1029, commonly called the credit card statute, but also covering telephone access codes, jurisdiction of the Secret Service can encompass local as well as interstate cases. Federal jurisdiction under the Computer Fraud and Abuse Act, Section 1030, is limited to situations in which "there is a compelling Federal interest, i.e., where computers of the Federal Government or certain financial institutions are involved, or where the crime itself is interstate in nature."[8] A memorandum between the Secretary of the Treasury and the Attorney General, signed in August 1985, designates that the FBI typically has primary jurisdiction for "1030" cases involving bank fraud, organized crime, national security, or terrorism, while the Secret Service has joint jurisdiction over other violations.

Negotiating the investigation and prosecution of multi-jurisdictional cases is difficult for several reasons. First, federal prosecution standards limit federal involvement in many of the computer-related offenses that come to the attention of state and county investigators. U.S. Attorneys decline to prosecute juveniles, which eliminates many "hacker" cases from their consideration, because the federal criminal justice system is not designed to handle juvenile matters. Cases involving adults are also declined if the dollar loss is not sufficient to meet federal prosecution requirements. Second, coordinating a set of local investigations is often handicapped because so few county and state investigators have knowledge about computer-related crimes. Even when investigators are willing to cooperate with each other, there is no guarantee that they will know enough about warrant preparation and evidence collection to prepare a good computer-related case.

Secret Service Efforts to Assist Locals

The Secret Service historically has been charged with the protection of the President of the United States, but other duties include investigations of crimes involving counterfeiting, forgery of U.S. obligations, access device fraud, computer fraud, and other specialized investigations.

The Service has a general policy of assisting local investigators in the investigation of computer-related crimes, even if the case results in a local prosecution, as long as the crime violates a federal law. Typically, a local investigator discovers a crime with federal implications and reports it to a local Secret Service field or resident office. (The Secret Service is staffed by 1,920 agents and has 62 field offices and 38 resident offices, located in state capitals, around the country. See Appendix F for a listing of these offices.) The Special Agent in Charge then determines whether the case appears to violate a federal law and whether the Secret Service will become involved. The U.S. Attorney decides whether to prosecute federally. In many cases there may be no one in the field office who has expertise in the investigation of computer-related crimes, but if the field office is willing to proceed with the case, it can contact

the Fraud Division in Washington, D.C. for support. The Headquarters is staffed with computer crime specialists who frequently assist field investigators. Headquarters often receives requests to transfer temporarily someone with experience in computer crime investigation into the requesting field office to assist in the collection of evidence or to assume responsibility for the case itself. It is also possible that the Secret Service will uncover a case unlikely to meet the U.S. Attorney's criteria for federal prosecution. In that event the Service is quite likely to assist in the local prosecution of the case. In some field offices (such as Philadelphia's) there are local law enforcement officers who work full-time at Secret Service locations, handling cases violating federal law but prosecuted locally.

At minimum, the Secret Service Headquarters serves as a technical resource and referral service for field agents who are confronted with the investigation of computer-related crimes. Agents at Headquarters are also prepared to handle the processing of evidence once it is collected in the field. The computer lab in Washington, D.C. has approximately ten personal computers and several printers. The Secret Service has purchased sophisticated equipment capable of disk conversion and other electronic media utility functions. With the increased level of sophistication of criminal activity, law enforcement will be challenged to keep pace. Special equipment will need to be acquired or developed to meet these demands. The Secret Service is preparing to address the challenge through development of a computer diagnostic facility.

Federal Bureau of Investigation Efforts to Assist Locals

Computer-related cases comprise a small percentage of the FBI's caseload: only about 100 of the more than 14,000 financial crimes reported annually involve computer-related incidents. Nearly half of those investigated in 1987 involved offenses by computer programmers and a third involved some form of telecommunications abuse. In that year 14 cases were closed, resulting in conviction of 73 individuals; seven cases presented for prosecution were declined by U.S. Attorneys.

Generally, the FBI will assist local investigators in the investigation of a computer-related offense only if the case involves a federal violation and is likely to be accepted for prosecution by the U. S. Attorney's office. In exceptional circumstances, even when a case does not meet the U.S. Attorney's guidelines, the FBI will ask for special consideration by the U.S. Attorney's office. When faced with an apparent federal case, local law enforcement personnel should contact the supervisor in charge of financial crimes in the nearest local FBI field office, who will be able to determine whether the offense qualifies as a federal violation. (Approximately 800 FBI Agents are assigned to the investigation of financial crimes. Not all of them are computer literate,

but of the 9,600 Special Agents in the entire organization, it is estimated that approximately 1,700 are. A list of field office locations is included in Appendix G.) Even if the offense does not meet the criteria set by the U.S. Attorney and the FBI chooses not to become involved, the financial crimes supervisor should be able to assist the investigation by referring the local investigator to computer experts.

The FBI's Laboratory Division at the Headquarters in Washington, D.C. formerly performed examinations of computer evidence for local and state law enforcement agencies upon request. Presently, the volume of FBI work precludes the lab's routinely offering the service to local law enforcement agencies. In extraordinary situations, such as in a recent local case in which computerized evidence was central to a homicide investigation, the lab may make exceptions to the policy, or may refer local agencies to other sources of support.

Interstate, Inter-County Cooperation

As more investigators and prosecutors become familiar with handling computer-related crimes, their ability to help each other in cases that cross jurisdictional lines will also increase. In many sites that are now investigating these kinds of crimes, it is not unusual for law enforcement officers to share expertise. Thus, for example, the Arizona Attorney General's office assisted the Columbus, Ohio Police Department so that a case with ties to both Arizona and Ohio could be prosecuted. In Colorado, most of the cases on which the Lakewood Police Department has assisted have occurred outside of Lakewood.

In order to be most successful, these arrangements should be formalized by networks of skilled investigators and prosecutors. Ideally these associations would have several layers—large local jurisdictions might have their own; state level associations could help to coordinate local efforts; and some participants in local and state chapters would communicate with the Federal Computer Investigations Committee (FCIC), the federal association that already exists. Federal coordination of these efforts would undoubtedly also be desirable to assure communication among the members.

Task Forces

Task forces can be useful in overcoming the difficulties of computer-related cases that involve several jurisdictions. Task forces generally include local and federal investigators and prosecutors. Usually they are formed by mutual agreement among the parties on an as-needed basis in cases that are very broad in scope. If a problem is persistent, a task force may be on-going. These arrangements allow the best minds to work together. A possible disadvantage may be that some will assist the task force without prosecuting the case in their jurisdiction.

In Arizona an ad hoc task force of state, local, and federal investigators and prosecutors recently has been formed to investigate a computer-related crime that spans federal and state jurisdictions. There can be a natural reciprocity in these types of cases: county and city staff can prosecute those cases that do not meet federal prosecution criteria, while federal prosecutors can facilitate multi-state investigations. Federal authorities can also obtain assistance from local investigators to avoid overextending federal resources.

Reporting Computer-Related Crime

Concerns of the Victim

One of the key difficulties in investigating and prosecuting computer-related crime is that many victims are reluctant to report or prosecute. In part, this may be because the limited number of law enforcement officers trained to investigate computer-related cases does little to inspire a victim's confidence in a public sector solution.[9] Many victims state that they do not report computer-related offenses because of unsatisfactory responses by law enforcement agencies to previous complaints.

From the victim's perspective, computer-related cases are complicated for several reasons. It may be unclear to the victim who should be contacted: in an interstate case, the FBI, the Secret Service, the U.S. attorney's office, and local prosecutors or law enforcement officers are all reasonable possibilities. Finding people who can help a company investigate a computer-related crime can be time consuming. Companies may lack confidence in the justice system and may not persist if help is not readily available.

Of course, victims, especially corporations, have a number of other reasons for hesitating to report computer-related crimes. In the book *How to Prevent Computer Crime: A Guide for Managers*, attorney and computer security analyst August Bequai discusses the following reasons for under-reporting of computer-related crime.[10]

- Prosecution is time consuming. Police often rely on the victim for assistance and his resources are limited. Operations may be affected as employees, records, and equipment may be used as witnesses or evidence.
- Corporations and victims of computer crime fear that the publicity will encourage others when the "tricks of the trade" are disclosed.
- Convictions are rare. Offenders often receive nothing more than a slap on the wrist. If convicted, computer criminals are often placed on probation or given a suspended sentence.
- Most computer crimes are viewed as civil rather than criminal offenses.

- Prosecutors are often more concerned with street crimes.
- The victim is often perceived by the public to be greedy, foolish, stupid, and careless.
- Victims fear that government investigations may reveal "management's dirty laundry."
- Corporations fear they may be liable for failing to establish adequate precautions and may face a stockholder lawsuit.
- Victims fear their insurance rates will rise or policies may not be renewed.
- Victims fear that their financial reputations may suffer.
- Victims may not prosecute for fear that their finances, marketing plans, trade secrets, or confidential information may be disclosed at the trial.
- Many statutes are difficult to apply to computer crimes.

The fact that victims of computer-related crime are especially sensitive to media coverage poses a difficult dilemma for investigators and prosecutors handling computer-related offenses. Although the threat of media coverage may dissuade many companies from reporting computer-related crimes, media coverage of successful prosecutions can improve the justice system's funding options for computer-related crime investigations, and may induce future victims to report computer-related crimes. Moreover some companies, like the telecommunications companies interviewed during this investigation, consider that media coverage can serve as a useful general deterrent.

Some commentators suggest that if law enforcement is to be effective in investigating and prosecuting computer-related crime, the law enforcement community will have to make stronger assurances of confidentiality than might otherwise be the case. They note that victims do not always wish to prosecute offenders, but would like to confer with law enforcement officers and prosecutors. By conducting confidential investigations, law enforcement can benefit from developing better statistics and an understanding of the various methods of operation than are now generated in lieu of confidentiality restrictions.[11]

Victim Vulnerability

The assistant Attorney General responsible for the prosecution of computer-related crimes in Ohio considers that the greatest handicaps to prosecuting computer-related crimes are that few computer-related crimes result in complaints and many of those that do are of such poor quality they cannot be prosecuted as computer crimes. He speculates that a portion of the explanation for underreporting is that many companies have such lax security

structures it takes the companies a long time to discover what has happened to them. Moreover the lack of effective security procedures often makes prosecution impossible. Considerations of employee privacy, freedom of movement, and a desirable working atmosphere may lead to inadequate procedures for protecting proprietary information. If a corporation does not inform employees in advance regarding what they cannot do, it is impossible to charge the employees later with having gained unauthorized access to information. Consequently it is much more difficult to prosecute computer-related crimes involving the theft of ideas (e.g., trade secrets, proprietary information) than the theft of property.

Investigators interviewed for this study advocated a corporate security plan including: a policy manual designating unauthorized use of computers; building security procedures; data security procedures; and computer security awareness training for employees, with a form signed by each employee indicating that the training has been received. These measures will not make companies invulnerable to computer-related violations, but they will enhance security.

Strategies for Involving Victims

The reporting of computer-related crimes can best be promoted by improved laws to address the needs of victims, by law enforcement officers and prosecutors trained to handle the investigation and prosecution of computer-related crime, and by efforts to inform potential victims of available prosecution options.

In Baltimore County, Maryland, the county police department involved the local police foundation, a group of approximately 20 local businesses that support excellence in law enforcement, in planning the department's computer crime unit. Not only did foundation members share important insights regarding the computer-related crimes occurring in the county, they also introduced the two detectives in the unit to community businesses that otherwise might never have known of the budding law enforcement capability.

Many investigators and prosecutors handling computer-related crime make special efforts to speak to local business groups, schools, and associations. These public appearances serve as forums for crime prevention, technology exchange, locating experts, and increasing the public's awareness of the criminal justice employees who are capable of addressing the needs of victims of computer-related crimes.

Many law enforcement officers who investigate computer-related crime also advocate the use of computer bulletin boards to improve law enforcement's awareness of the crime and the public's awareness of law enforcement's interests and capabilities. They list a number of advantages to running a

bulletin board system: it helps to develop a network of informants; it connects law enforcement officers who are interested in computers; it can be good for public relations; it is very useful for intelligence gathering in all sorts of offenses (e.g., regarding burglaries, drug crimes, and right-wing extremist activities); and use of the board can lead to opportunities for public speaking.

Equipment Concerns: Low Tech Solutions to High Tech Crimes

Commonly, law enforcement and prosecutors' offices lack the automation of the private sector. On a door in the Arizona District Attorney's Office, there is a sign that reads, "Low Tech Solutions to High Tech Problems," highlighting the serious technological disadvantage that many employees of criminal justice agencies suffer when addressing computer crime. Consequently, it is not surprising that when the need for a computer crime investigator or prosecutor arises, it is difficult to find anyone with the expertise to tackle the task. Law enforcement is faced with needing both equipment and people who are skilled to operate that equipment to improve their effectiveness in general, and to be competitive in the area of computer-related investigation and prosecution in particular.

The absence or minimal use of computers in many law enforcement and prosecutors' offices is both a symbol and a symptom of a critical problem for investigators and prosecutors. It suggests how little computers are being considered by justice officials and underscores how far behind the criminals many offices have become. It may also reduce the likelihood that individuals with technical skills will be employed or, at least, recognized in those justice settings.

A simple solution, though not necessarily simply implemented, is for law enforcement and prosecutors' agencies to install as many micro-computers in their agencies as budgets will allow. An agency should realize many rewards from such a strategy. For one, existing personnel will likely become computer literate, which would improve their ability to handle computer-related crimes. Also, the chances of recruiting persons with computer skills would increase. The agency might even be appealing to a person with strong technical skills who could oversee the use of the computers and be an expert advisor to investigations of computer-related crime. As a third benefit, the agency would have access to the expanding collection of computer software aimed at managing criminal justice caseloads, training justice personnel, and analyzing justice information.

There are other needs for equipment to improve the investigation of computer-related crimes as well. In Arizona, it is difficult for the Attorney

General's office even to have access to sufficient numbers of DNRs. (Ironically, these are already becoming obsolete as criminals use cellular phones and even more sophisticated equipment to commit their crimes.) In Philadelphia, detectives in the economic crime unit cannot run a computer bulletin board because they have neither a micro-computer nor a modem. Indeed, the following list of equipment and services needed for the investigation of computer-related cases, which was recommended by advisors to this project, is quite extensive.

Several desktop and laptop computers to comprise a micro-computer lab

Communications protocol analyzers

Recording modems

Tape streamers (for backup)

Magnetic media safe storage facilities

Audit software (e.g., comparison utility)

Utilities disks (e.g., Norton utilities, Ultra utilities and others)

Computer services subscriptions to such companies as CompuServe

Access to Dockmaster (operated by the National Computer Security Center of the NSA) and other electronic bulletin board systems

Standard equipment: cameras, labels, phones - two direct dial types for use with modems

DNRs/pen registers

Computer manuals

Air conditioned (cool) building with an uninterruptable power source

Training

Almost everyone addressing the problem of computer-related crime agrees that investigators and prosecutors need training. The nature and extent of the training depends on the needs of the agency, but there is little question that there is currently only a handful of people with enough knowledge about computers and the investigation and prosecution of computer-related cases to do those jobs well.

Nearly every agency could benefit from having some or all personnel receive general awareness training, introducing the trainees to computers and their use in the commission of computer-related crime. If an agency is small it

may not be necessary for many persons to receive this kind of training, but agency policy should require that those with computer expertise be contacted in all computer-related investigations or prosecutions. In large agencies, where there may be considerable specialization, it is important that several people have received awareness training. In the New York City Police department, for example, a division of officers acts as crime scene investigators. Given the complexities of computer-related evidence collection discussed earlier, it would be critical that these individuals receive awareness training, as well as those who will conduct the more detailed aspects of computer-related investigations.

Some agencies also have caseloads that will warrant having certain people receive expert training. That training would certainly involve a number of technology issues not touched upon in the general awareness course as well as a review of specific investigation problems using several case studies. In addition since computer technology is changing rapidly, expert training will undoubtedly need to be a routine part of in-service training for certain individuals.

Unfortunately training in the investigation and prosecution of computer-related crime is not easy to find or afford, but courses can be found at the federal, state, and county levels, provided by both public sector and private organizations.

Federal Government Sources

Courses in computer-related crime are offered at both the FBI training academy in Quantico, Virginia and the Department of the Treasury's Federal Law Enforcement Training Center in Glynco, Georgia. Each has a limited number of openings for local law enforcement personnel, but waiting lists for both curricula are quite long. Both have the capability to conduct "roadshow" training sessions; in fact the FBI does offer five to ten roadshows per year. But as currently configured, neither program could easily meet the demand for training at the local level.

The U.S. Secret Service is developing an intensive two-week computer fraud training course designed to benefit both investigative agents and technical support personnel. The course will be offered initially only to Secret Service personnel, however, because it is designed to meet specific jurisdictional requirements.

The National College of District Attorneys in Texas offers a five-day forensic evidence course, which includes a one and a half hour component on computer crime prosecution. The component is generally included every other year, depending on demand. The College has also conducted "roadshow" training, although not in the area of computer-related crime.

State and Local Law Enforcement Training

Given the limited travel funds available in most agencies, the need for a number of people to receive training, and the need for in-service training, in-state training is a desirable solution. One way to accomplish this is for a number of agencies to request "roadshow" assistance from existing federal training sources. Another option may be to find talented agency personnel who can provide suitable training. States and counties with local computer crime associations have adopted this strategy, combining the skills of their public and private sector members to develop training for law enforcement officers, prosecutors, and judges (if interested) in courses on computer-related crime. In some states, training in computer crime investigation is available through training academies.

Private-Sector Sources

Consultants can also be hired to provide computer-related training. In Ohio, a firm called Adaptive Systems, Inc. contracts with the Ohio Peace Officer's Training Council to provide training in computer-related crime investigation. The Training Council oversees the training in computer-related crime investigations; a full-time trainer at the Ohio Peace Officer's training Academy coordinates the training provided by Adaptive Systems. Adaptive Systems in turn engages local law enforcement officers, private security personnel, and prosecutors to give lectures in certain areas. Because the Academy does not have its own computer equipment Adaptive Systems also provides equipment for the course. A key advantage to contracting for training with a local consultant, rather than one who travels to a site, is the possibility for on-going support services.

An instructor from the Federal Law Enforcement Training Academy, who is also a private investigator, has acted as a training consultant for a number of departments. As an example, the police department in St. Petersburg, Florida, hired him to teach a course on computer-related crime investigation and then recruited participants from their own and neighboring departments.

Private companies have also provided free training to law enforcement. In Arizona high tech firms have been known to provide seminars and invite law enforcement at no cost. Telecommunications companies are also prepared to assist with training in the investigation of telecommunications fraud. In August 1988, the Baltimore County police department and the Communications Fraud Control Association sponsored a one-day training seminar on telecommunications fraud investigations for law enforcement officers in Maryland.

An assistant district attorney in Middlesex County, Massachusetts, suggests that law enforcement formalize a training relationship with the private sector by forming what he terms a "high-tech" chamber of commerce. The

chamber would support high-tech training for local law enforcement, and much like the police foundation does in Baltimore County, Maryland, it would serve as a liaison between law enforcement agencies and the business community.

A list of computer-related training sources is provided in Appendix H.

Recruiting and Keeping Computer-Literate Staff

In most cases, expertise in computer-related investigations and prosecutions results when individual investigators and prosecutors with an interest in computers seek the challenge of handling those cases. Unfortunately that sort of ad hoc structure can have a number of flaws. The greatest weakness is that the ability to handle computer-related investigations and prosecutions then rests solely with the individuals who do the job. When those individuals leave, the function can leave with them. Without support from the top of an organization, recruitment of new, technically adept personnel often does not occur. In Philadelphia and Denver, when the prosecutors who handled computer-related crimes accepted positions outside the district attorney's offices, no effort was made to replace them with people with interest and skills in computer-related prosecution. In Maricopa County, the Sheriff's office's computer crime unit, once a two-person operation, has been staffed by one person for more than two years.

Moreover, without interest at the Chief, Sheriff and District Attorney levels, there may not be enough support for the painstaking nature of computer-related investigation to assure that good people stay. Because the processing of violent offenses overshadows other investigations and prosecutions, law enforcement officers are able to investigate computer-related crimes only if they also fulfill a host of other functions in the office. Some oversee the computer systems, while others maintain a standard caseload and handle computer-related cases virtually on their own time. Many prosecutors get bogged down with a heavy caseload of traditional economic or organized crime cases that reduce their effectiveness on the computer-related ones. In Lakewood, the detective who handles computer-related crimes is now charged with working a regular caseload including conducting vice and narcotics investigations, handling video surveillance, and executing wire taps. But leadership in the Lakewood Police Department is very anxious to increase the detective's ability to monitor computer issues. In spite of serious budget constraints, the department is working to create a technical position that he will fill. The duties of the position would be exclusively technical and include such things as managing data banks, programming, overseeing the departments micro-computers and executing wire taps. The detective would then continue to be the technical assistant in computer-related cases, without the added burden of unrelated investigative responsibilities.

Leadership is also necessary to assure innovative opportunities for promotion. In most law enforcement agencies, promotion for computer crime investigators means a return to patrol, quite possibly a less appealing option than employment in the private sector. Recruitment is another problem requiring an innovative solution. In most law enforcement agencies individuals serve considerable time on patrol before being considered for investigative opportunities. People with an interest and training in computers, however, are likely to be among the newer members of an agency. Ways to create opportunities for those individuals to share their talents, without diluting the quality of computer-related investigations, must be considered. Civilians can also be considered to provide technical assistance. Prosecutors offices may actually want to recruit individuals from the private sector with an interest in computer-related prosecutions.

Of course, the extent to which an agency can afford to encourage specialization will depend on its size, budget, and caseload. The point is that individuals who investigate and prosecute computer-related cases will be more productive and remain longer if agency leadership is prepared to recognize and reward the development of computer-related skills.

Finding Experts

Investigators and prosecutors who handle computer-related crimes often require assistance from technical experts. In addition to the strategies for locating experts discussed in Chapter III, private sector resources may be considered. Professional associations, many with state chapters, could be helpful, including the American Society for Industrial Security, the Association of Electronic Data Processing (EDP) auditors, and the Communications Fraud Control Association. (More complete references and additional organizations are listed in Appendix C.) Technical universities and even local high schools may have instructors who can provide assistance with the technical aspects of computer-related cases. Vendors can also be helpful. Vendors have provided law enforcement officers with brief, hands-on training during the course of investigations. They have also been helpful in retrieving data from computer disks that initially appeared empty.

The problem with many private sector experts, however, is cost. The assistant Attorney General in Arizona commented that she often needs experts, but cannot always find or afford them. It can cost as much as $3,000 to $5,000 for expert assistance on a relatively simple case. Hence, the cost of experts may be the single greatest incentive for establishing as much expertise within criminal justice agencies as possible.

State-level Involvement in Investigation, Prosecution, and Program Development

In states in which jurisdiction and budgets allow state-level organization of teams of expert investigators and prosecutors, there are obvious benefits for local jurisdictions—especially those with limited resources. In those settings, local investigators and prosecutors can have sole responsibility for collecting evidence and prosecuting relatively uncomplicated computer-related cases. State experts can be called upon to assist in, or assume responsibility for, more difficult investigations and prosecutions. At minimum, state experts can provide significant training support to persons in local jurisdictions.

Arizona, Illinois, and Ohio have developed capabilities within their state governments to investigate computer-related crime. As noted throughout this report, the Arizona Attorney General's office investigates and prosecutes complicated computer-related cases occurring in the state. The office also conducts regular training sessions for local law enforcement agencies around the state. In Illinois the state police have a computer crime unit which, in addition to investigating computer-related crimes, is developing a training program for local law enforcement agencies in the state. Recently, the Ohio Attorney General's office hired an attorney charged with developing a statewide computer crime task force that will function as a technical resource and training hub for law enforcement and prosecutors' agencies in the state.

Investigation and/or prosecution by state agencies is not a viable option in all states. A recent survey revealed that only about half of state law enforcement agencies have investigative powers that would support the creation of computer crime units.[12] Additionally, only about half of state attorneys general are empowered to prosecute cases at the trial level, while considerably fewer than half actually do.[13] But even if state governments cannot play a major role in the investigation and prosecution of computer-related crime, they can still support improved investigation and prosecution. Some activities might be well-suited to state- level criminal justice coordinating bodies if they exist.

States can set training standards that include instruction in computer-related crime and, where appropriate, assure on-going, in-state training of investigators and prosecutors. Where there are state-level training bodies, those organizations can assume a major role in evaluating the needs for computer-related training, investigating the various methods for providing it, and assuring that base-level and in-service courses are available. In states in which those types of organizations do not exist, state-level associations of Sheriffs, Chiefs of Police, and District Attorneys could be called upon to fulfill those functions.

States can also provide a forum for the sharing of information regarding computer-related investigation and prosecution. An association of local

investigators, prosecutors, and experts to share information relating to computer-related crimes might be organized at the state level. In turn combined state associations might form a national chapter of persons who handle computer-related crime at the state and local levels. State associations could serve as a resource for all jurisdictions in the state that might require support during the investigation and prosecution of computer-related crime and as a repository of information on expert assistance and developing technology. Those associations might also assume a central role in strengthening relationships among the private and public sectors.

Finally, states can stimulate the development of local capabilities to investigate and prosecute computer-related crime by authorizing development grants to local jurisdictions. Appropriate areas of state support could include acquisition of needed equipment, software, and training.[14]

Endnotes

1. See J. Thomas McEwen, et al., *Dedicated Computer Crime Units* (Washington, D.C.: National Institute of Justice, 1989) for a detailed discussion of state laws.
2. Richard C. Hollinger and Lonn Lanza-Kaduce, "The Process of Criminalization: The Case of Computer Crime Laws, " *Criminology*, Vol. 6, No. 1 (1988): 103.
3. Douglas H. Reimer, "Judicial and Legislative Responses to Computer Crimes," *Insurance Counsel Journal* (July 1986): 335; Michael Rostoker and Robert H. Rines, *Computer Jurisprudence: Legal Responses to the Information Revolution* (New York: Oceana Publications, Inc., 1986): 419.
4. Rostoker and Rines, *supra*, note 3, at 340-341.
5. Hollinger and Lanza-Kaduce, *supra*, note 2, at 103-104.
6. Hollinger and Lanza Kaduce, *supra*, note 2, at 104.
7. 18 U.S.C. 1029; 18 U.S.C. 1030, as amended by PL 99-474 in 1986.
8. Computer Fraud and Abuse Act of 1986, P.L. 99-474, Senate Report No. 99-432, p. 2482.
9. August Bequai, "Technocrimes—Why the Cops Can't Cope," *Law Enforcement Technology* (March/April 1987): 28.
10. August Bequai, *How to Prevent Computer Crimes: A Guide for Managers* (New York: John Wiley and Sons, 1983): 46.
11. James Conser and Louis Carsone, "The Role of Law Enforcement in Computer Crime and Computer Security," Chapter 1 in *Microcomputers in Criminal Justice: Current Issues and Applications* (Cincinatti, Ohio: Anderson Publishing Co., 1987):8.
12. Peter Finn, Daniel McGillis, and Richard Sinnot, *State Law Enforcement: A Survey of Major Services*, draft (Cambridge, Mass.: Abt Associates, February 1988).
13. U.S. Department of Justice, Law Enforcement Assistance Administration *State and Local Prosecution and Civil Attorney Systems* (Washington, D.C.: GPO, 1978).
14. This idea was communicated by James Conser in a letter to the author.

Chapter VI: A Strategy for Improving the Investigation and Prosecution of Computer-Related Crime

The aim in this section is to provide a strategy that jurisdictions can consider when planning to address the problem of computer-related crime. Whether a particular jurisdiction implements some or all of the strategy will depend on its size, the budgets of its criminal justice agencies, and the nature of the community served by those agencies.

The experiences of the sites contacted for this study suggest that because there are currently so few individuals capable of investigating and prosecuting computer-related crime, the need to pool resources will continue for a number of years. Hence a set of core elements is proposed here that includes coordination of resources within an agency, among agencies, and with the community. At present the elements appear important for agencies of all sizes.

Core Elements

1. Make a commitment to be responsive to the victims of computer-related crime.

If the handling of computer-related crime is to be improved, the highest level officials (Chiefs of Police, Sheriffs, and District Attorneys) must make a commitment to establish the capability to address that crime.

2. Determine the level of commitment that is feasible.

This will determine how far in the process an office or department is prepared to go. Computer management specialist James Conser suggests the following grid for assisting agencies in determining their level of investment in computer-related crime investigation and prosecution.[1]

STRATEGY FOR HANDLING COMPUTER-RELATED CRIME

Agency Size	Shared Resources	Functional Specialist	Full-time Assignment
Small	H	L	N/R
Medium	M	H	L
Large	L	M	H

N/R = Not Recommended
L = Low Recommendation
M = Moderately Recommended
H = Highly Recommended

Conser defines the strategies as follows:

Shared Resources
- personnel
- intelligence
- knowledge/information
- task forces and joint assignments
- regional, county, and/or state resources

Functional Specialist
- developing expert investigative skills and techniques to be employed only when necessary; not a full-time agency assignment

Full-time Assignment
- investigator(s) assigned computer-related cases on a full-time basis

3. Conduct a skills and interests survey and identify at least one investigator and one prosecutor (possibly those with skills in handling economic crimes) with an *interest* in computer-related crime.

If no one is identified, begin reviewing the credentials and interests of all prospective candidates.

4. Assure that the individual(s) receive at least base-level training.

This will mean participating in courses available at the federal level, if feasible, but will likely also mean one or more of the following: working with state-level chief's, sheriff's and prosecutor's associations to lobby for an ongoing intra-state training program; altering local/state recruit and in-service training curricula to include computer-related crime; lobbying to expand the "roadshow" capabilities of the federal government's training programs; reviewing the possibility of hiring consultants, then sharing costs across several departments; and/or providing training through a local association of investigators and prosecutors who investigate and prosecute computer-related crimes. The goal should be to have at least one trained staff person and training resources available for refreshing and updating information.

5. Establish operating procedures or organizational reporting requirements to assure that the person who is trained to handle computer-related cases is known to all others in the office and that the person is consulted whenever a computer is involved in a case.

6. Identify technical support resources.

The first step in this effort should be to determine whether there is a staff person (not necessarily an investigator or prosecutor) with technical computer skills who could assist in the investigation/prosecution of computer-related crimes. In the case of law enforcement, that person could be a civilian or sworn officer who would provide as-needed assistance to the technical aspects of collecting and reviewing evidence.

The second phase of the effort will be to supplement the investigative expertise within the office with technical experts and investigators in the community, and others at the local, state, and federal levels (e.g., other law enforcement officers and prosecutors (including those at the federal level), electronic data processing (EDP) auditors, local universities, vendors, and reserve officers). The intention is to establish a reserve of technical experts to assist with investigating and prosecuting computer-related crimes before those crimes are reported.

7. Where feasible, coordinate law enforcement and prosecution efforts.

The important point is to ensure that people who will ultimately work together begin working together from the outset.

8. Where possible, work closely with other law enforcement officers and prosecutors to form a local and/or state association of computer-related crime investigators and prosecutors.

These types of associations can provide a significant investigative resource and can also play a major role in providing regional and/or statewide training. Associations will prove especially helpful to smaller departments and offices, because larger departments and offices are likely to have more reported cases and therefore more experience dealing with the range of computer-related cases. (Existing examples of county, state and federal associations are LEETAC, CACCI, and FCIC. See Appendix C for more details.)

9. Involve potential victims in the effort.

Allow time for public speaking engagements with businesses, schools, and agencies to increase potential victims' awareness of the justice system's attention to the issue. The effort will likely identify cases that have gone unreported, thereby supporting the need for the investigative and prosecution capabilities, and should increase the likelihood of future reporting. It may also serve a crime prevention function by making companies more aware of protective measures. Many people have commented on the need to educate computer science students about the ethical and legal issues

connected with using computers. In addition, a number of investigators and prosecutors have found that they can make businesses aware of their vulnerability to computer-related crime and can develop important ties with potential victims by engaging in public speaking activities. Investigative and prosecution agencies that already participate in considerable community relations activities should consider including computer-related crime among the topics presented as part of those activities.

Optional Capabilities

Implementation of the strategies suggested here will depend greatly on resource flexibility and need. Note that need may increase with time, so review of these options should occur annually, especially in growing departments or offices.

1. Establish a team of investigators and prosecutors with exclusive responsibility for computer-related crimes, and limit other investigative and prosecution responsibilities.

There are undoubtedly several ways to organize these sorts of teams. The officer in Columbus, Ohio who handles computer-related offenses considers that the ideal investigative unit should consist of at least two investigators, with as many as five persons for the investigation of complicated crimes. One person should be an administrator who could oversee investigations, another would be a programmer/analyst who might work part-time on investigations of computer-related crimes and part-time supporting more general programming needs in the office; a third would be a lab technician who is familiar with a variety of hardware and software and can serve as an evidence expert at the crime scene and at trial. These three might have other responsibilities within the department as well. The team would be completed by one or two investigators responsible for interviewing and interrogating witnesses and victims of computer-related crimes. In addition, the team would require some physical accommodations and supplies.

The assistant Attorney General in Arizona can envision keeping one attorney and two investigators busy at all times. She could see such a team functioning as a technical resource group that would assist not only in the investigations/prosecutions of computer crimes per se, but also in the prosecution of other types of cases in which computers are involved. The investigators could be responsible for such things as wire taps, computer searches, and litigation support, i.e., managing and indexing evidence. She also suggests that were the office automated a technical computer person could share his or her services when there was the need to prepare search warrants and review evidence.

As noted in the introduction to this report, a separate report focusing on dedicated computer crime units is available.

2. Develop a technical staff (not necessarily dedicated to the investigation of computer-related crime, but who can support that kind of investigation).

As law enforcement and prosecutors agencies increase their level of automation, they will need technical personnel who can oversee and maintain the office computer systems. Those individuals can also support some of the technical aspects of investigating and prosecuting computer-related crime. Finding those individuals may not require the agency to hire additional personnel. As noted earlier, the police department in Lakewood is working to increase the technical responsibilities of the investigator responsible for computer-related crime so that he can provide a range of technical services to the department.

3. Obtain expert and in-service training for specialists within a department or office.

Changes in computer technology and the ways criminals use computers to commit crimes occur almost daily. Persons investigating and prosecuting a substantial volume of computer-related cases will need continued training in the subject. Persons who have received expert training can also be an important training resource for others in the agency. If a local or state association of investigators and prosecutors is formed, experts can also share their training with other agencies throughout the local jurisdiction or state.

Ideally, training would be provided locally or regionally, but if the number of people who need expert training is not sufficient to warrant offering or purchasing it on-site, agencies may want to consider sending experts to one of the existing federal programs for advanced training. Additional computer training provided by private sector companies may also need to be considered.

4. Assure base training in computer-related crime investigation/prosecution for all officers/prosecutors, or at least those involved in crime scene work and screening.

The variety of ways in which computers can be used in the commission of crimes suggests that, especially in large agencies, many investigators and prosecutors not assigned to handle computer-related crimes will be confronted with computer evidence. Because it may not always be possible to consult with departmental experts, it would be helpful if at least those investigators involved in crime scene work and prosecutors who screen incoming cases receive base-level training in handling a computer-related case.

Cases can then be turned over to the appropriate experts without fear of losing or contaminating valuable evidence.

5. Purchase equipment (or obtain it through forfeiture or donation).

Ready access to computer equipment is needed to analyze computer-related evidence and present it in court. Investigators cannot always rely on support from victim companies, so law enforcement and prosecutors agencies prepared to develop more than minimal expertise in the investigation of computer-related crime will have to obtain some computer equipment.

Almost every law enforcement agency currently involved in investigating computer-related cases has used state forfeiture provisions to obtain computer equipment. In addition, it may be possible to interest private businesses in making equipment contributions. In micro-computer cases involving the Secret Service, it may also be possible for a local agency to receive support from the Service, which has equipment that can convert floppy disks from different types of micro computers to ones that are readable by a generic computer likely to be available to a number of investigators.

6. Lobby for state and federal coordination of investigation and prosecution efforts, including the sharing of investigation and prosecution resources, technology, and training.

Currently there are few investigators and prosecutors who have handled computer-related cases, so there is considerable need to share knowledge and resources. As discussed in Chapter V, the fact that computer-related cases often involve multiple jurisdictions may require a team approach to their investigation and prosecution. Response can be improved by developing procedures for coordinating efforts before a multi-jurisdiction case occurs. State and federal governments could be critical to improving local investigation and prosecution by: providing financial incentives for local government to develop expertise in computer-related investigation and prosecution; helping to centralize information on investigation and prosecution resources; providing training, coordinating local activities through state and federal associations; and providing information on technological developments likely to affect the prosecution and investigation of computer-related crime.

Endnotes

1. This grid was communicated by James Conser in a letter to the author of this report.

REFERENCES

American Bar Association. *Counterfeit Committee Report.* Washington D.C., 1982.

American Bar Association. Task Force on Computer Crime, Criminal Justice Section. *Report on Computer Crime.* Washington, D.C., 1984.

Archambeault, William G. and Betty J. Archambeault. *Computers in Criminal Justice Administration and Management: Introduction to Emerging Issues and Applications.* Cincinnati: Anderson Publishing Co., 1984.

Arkin, Stanley, et al. *Prevention and Prosecution of Computer and High Technology Crime.* New York: Matthew Bender and Co., 1988.

Bequai, August. *Computer Crime.* Lexington, MA: Lexington Books, 1978.
Bequai, August. *How to Prevent Computer Crime: A Guide For Managers.* New York: John Wiley and Sons, 1983.

Bequai, August. *Technocrimes.* Lexington, MA: Lexington Books, 1987.

Bequai, August. *Technocrimes—The Computerization of Crime and Terrorism.* Lexington, MA: Lexington Books, 1986.

Bequai, August. "Technocrimes—Why the Cops Can't Cope." *Law Enforcement Technology.* March/April 1987: 28.

Bequai, August. *White Collar Crime.* Lexington, MA: Lexington Books, 1977.

Blackwell, Angela Glover, Lois Salisbury, and Sidney M. Wolinsky. *Petty Larceny: Excessive Bank Charges Produce Banking Crisis For The Poor.* An Administrative Petition to Ensure Essential Banking Services for all California Consumers. Public Advocates, Inc., San Francisco.

BloomBecker, Jay. *Computer Crime, Computer Security, Computer Ethics—First Annual Statistical Report of the National Center for Computer Crime Data.* Los Angeles: National Center for Computer Crime Data, 1986.

BloomBecker, Jay. *Computer Crime Law Reporter: 1986 Update.* Los Angeles: National Center for Computer Crime Data, 1986.

BloomBecker, Jay. "Computer Crime Update: The View as We Exit 1984." *Western New England Law Review* 7: 627-49.

Compendium of Data Processing and Telecommunications Training Courses for Auditors and Investigators. President's Council on Integrity and Efficiency. Computer Commitee, 1986.

Computer-Related Crime: Analysis of Legal Policy. Paris: Organization for Economic Co-Operation and Development, 1986.

Computer Security Handbook—The Practitioner's Bible. Northborough, MA: Computer Security Institute, 1985.

Conser, James A., Louis P. Carsone, and Robert Snyder. "Investigating Computer-Related Crimes Involving Small Computer Systems." In Palmiotto, Michael, ed. *Critical Issues in Computer Investigation 2nd Edition.* Cincinnati: Anderson Publishing Co., 1988.

Cooper, J. A. *Computer-Security Technology.* Lexington, MA: D. C. Heath and Company, 1984.

Davis, Bob. "Abusive Computers." *The Wall Street Journal.* CCX 37 (August 20, 1987): 1.

Executive Training and Development Sources: Compendium for Offices of Inspector General. President's Council of Integrity and Efficiency, 1985.

Federal Computers and Telecommunications, Security and Reliability Considerations, and Computer Crime Legislative Options. Prepared for the Office of Technology Assessment, Washington D.C. by Data Security Systems, Inc. Natick, MA, 1985.

Finn, Peter, Daniel McGillis, and Richard Sinott. *State Law Enforcement: A Survey of Major Services.* Draft. February, 1988.

George, B. J. "Contemporary Legislation Governing Computer Crimes." *Criminal Law Bulletin.* 21(5): 389-412.

Gish, J. "Computer Crime and Punishment—The View From the DA's Office." *Information Strategy—The Executive's Journal.* 1(2):11-15, 17.

Glazer, Alan. "CCTV: Advances In Security Systems." *Law Enforcement Technology.* March/April 1987: 34.

Goldstein, Mark L. "Time to Lock the Door: High-Technology Fraud is Now Big Business." *Industry Week.* June 29, 1987: 58-61.

Hollinger, Richard C., and Lonn Lanza-Kaduce. "The Process of Criminalization: The Case of Computer Crime Laws." *Criminology* 26(1): 101.

Ingraham, Donald G. "On Charging Computer Crime." *Computer/Law Journal* 2: 429-39.

"Insurers Grapple with Con Men in War Against Fraud." *Reliance Reporter.* 4(3): 4-6.

Kling, Rob. "Computer Abuse and Computer Crime as Organized Activities." *Computer/Law Journal.* 2(2): 403-427.

Kutz, Robin K. "Computer Crime in Virginia." *William and Mary Law Review.* 27(783): 783-831.

Landis, Dylan. "Insurance Fraud: Billions in Losses." *The New York Times.* July 6, 1982: D1.

Landreth, Bill. *Out of the Inner Circle. A Hacker's Guide to Computer Security.* Bellevue, Washington: Microsoft Press, 1985.

Loebel, Jerome. *Foiling the System Breakers: Computer Security and Access Control.* New York: McGraw-Hill, 1986.

Marx, Gary, and Sanford Sherizen. "Monitoring on the Job: How to Protect Privacy as Well as Property." *Technology Review* November/December, 1986: 63-72.

McEwen, J. Thomas et al. *Dedicated Computer Crime Units.* Washington, D.C.: National Institute of Justice, 1989.

Millard, C. J. *Legal Protection of Computer Programs and Data.* England: 1985.

Molnar, Jack. "Putting Computer-Related Crime in Perspective." *Journal of Policy Analysis and Management.* 6(4): 714-716.

Moultan, R. T. *Computer Security Handbook—Strategies and Techniques for Preventing Data Loss or Theft.* Englewood Cliffs, NJ: Prentice-Hall, 1986.

Parker, Donn B. "Computer Abuse Research Udate." *Computer/Law Journal* 2: 329-52.

Parker, Donn B. *Computer Crime: Criminal Justice Resource Manual.* Washington, D.C.: National Institute of Justice, 1989.

Parker, Donn B. "Computer-Related White Collar Crime." In Geis, Gilbert, and Ezra Stotland, eds. *White Collar Crime: Theory and Research.* Beverly Hills: Sage, 1980.

Parker, Donn B. *Crime by Computer.* New York: Charles Scribner's Sons, 1976.

Parker, Donn B. *Fighting Computer Crime.* New York: Charles Scribner's Sons, 1983.

Parker, Donn B. *How Much Computer Abuse Is There?* Menlo Park, CA: SRI International, 1981.

Perry, R. L. *Computer Crime.* New York: Franklin Watts, Inc., 1986.

Purdy, Stephen R. *Computer Crime Investigations.* Draft monograph. Federal Computer Investigations Committee, 1988.

Report of the National Commission on Fraudulent Financial Reporting. Washington, D.C., 1987.

Reimer, Douglas M. "Judicial and Legislative Responses to Computer Crimes." *Insurance Counsel Journal.* July, 1986: 406-430.

Ross, S. J., R. H. Courtney Jr., D. B. Parker, W. H. Murray, and P. B. Wild. "Computer Security Issues—A Roundtable." *Computer Security Journal.* 3(2): 39-50.

Rostoker, Michael D. and Robert H. Rines. *Computer Jurisprudence: Legal Responses to the Information Revolution.* New York: Oceana Publications, 1986.

Sanger, David E. "S.E.C.'s Computer Revolution." *The New York Times.* April 1, 1987: D1.

Schemann, Serge. "German Computer Hobbyists Rifle NASA's Files." *The New York Times.* September 16, 1987.

"Sharper Sleuthing Plus Tougher Sentences: Potent Rx in War Against Insurance Fraud." *Reliance Reporter.* 4(4): 2-3.

Sherizen, Sanford. *Criminological Perspectives on Major Aspects of Computer Crime Behaviors.* Abstract of paper submitted for consideration for the 10th National Computer Security Conference, 1987.

Sherizen, Sanford. *Federal Computers and Telecommunications-Security and Reliability Considerations and Computer Crime Legislative Options.* Natick, MA: Data Security Systems, Inc., 1985.

Sherizen, Sanford. "Moving Toward Mandatory Data Security." *Computerworld.* November 18, 1985: 17.

Sherizen, Sanford, and Gary Marx. "Technology: Invader or Protector of Privacy?" *Computerworld.* July 20, 1986: 60.

Sieber, Ulrich. *The International Handbook on Computer Crime.* New York: John Wiley and Sons, 1986.

Sloan, Irving J. *The Computer and the Law.* New York: Oceana Publications, 1984.

A Small Business Guide to Computer Security. Pamphlet. Washington, D.C.: Small Business Administration, 1987.

Soma, John T., Paula J. Smith, and Robert D. Sprague. "Legal Analysis of Electronic Bulletin Board Activities." *Western New England Law Review* 7: 571-626.

Somers, L. E. *Economic Crimes—Investigative Principles and Techniques.* 1984.

Southard, Douglas K. "To Catch a Thief: Criminal Law is Catching Up With High Tech's Information Thieves." *California Laywer.* December, 1986: 23-25.

Thackeray, Gail. "Problems of Computer Evidence." In *The Practical Prosecutor.* National College of District Attorneys, Houston. Volume 1985 (2): 10-11.

Tien, James M., Thomas F. Rich, and Michael F. Cahn. *Computer Crime: Electronic Fund Transfer Systems Fraud.* U.S. Department of Justice. Bureau of Justice Statistics. Washington, D.C., 1985.

Tompkins, Joseph B., and Linda A. Mar. "The 1984 Federal Computer Crime Statute: A Partial Answer To A Pervasive Problem." *Computer/Law Journal.* 6: 459-483.

Training and Development Sources Guide: Compendium of Existing Courses/Lessons, Offices of Inspector General. President's Council on Integrity and Efficiency. Washington, D.C., 1982.

Trew, Andrew. "Does Technology Outstrip Enforcement?" *Computer Law and Practice.* July/August, 1986: 178-181.

U.S. Congress. House. Small Business Committee. Subcommittee on Regulation and Business Opportunities. *Testimony of Peter S. Browne,* Chairman, Small Business Computer Security and Education Advisory Council. 100th Cong. 1st Sess., November 16, 1987. Serial 100-38.

U.S. Department of Health and Human Services. Office of the Inspector General. *Computer-Related Fraud and Abuse in Government Agencies.* Washington, D.C., 1983.

U.S. Department of Health and Human Services. Office of the Inspector General. *Computer-Related Fraud and Abuse in Government Agencies: Perpetrator Interviews.* Washington, D.C., 1985.

U.S. Department of Justice. Bureau of Justice Statistics. *Computer Crime: Criminal Justice Resource Manual.* Washington, D.C., 1979.

U.S. Department of Justice. Bureau of Justice Statistics. *Computer Crime: Computer Security Techniques.* Washington, D.C., 1979.

U.S. Department of Justice. Bureau of Justice Statistics. *Computer Crime: Electronic Fund Transfer Systems and Crime.* Washington, D.C., 1982.

U.S. Department of Justice. Bureau of Justice Statistics. *Computer Crime: Expert Witness Manual.* Washington, D.C., 1980.

U.S. Department of Justice. Bureau of Justice Statistics. *Electronic Fund Transfer and Crime.* Washington, D.C., 1984.

U.S. Department of Justice. Law Enforcement Assistance Administration. *State and Local Prosecution and Civil Attorney Systems.* Washington, D.C., 1978.

U.S. Department of the Treasury. *Computer Fraud/Data Processing Investigations Training Program.* Syllabus. Federal Law Enforcement Training Center. Glynco, GA, 1986.

U.S. Department of the Treasury. *White Collar Crime Training Program.* Syllabus. Federal Law Enforcement Training Program. Glynco, GA, 1985.

U.S. General Accounting Office. *System Integrity: Stronger Controls Needed for Customs' Automated Commercial System.* Report to the Commissioner of the U.S. Customs Service. Washington, D.C., 1987.

Waal, P.C. "Keeping Hackers at Bay." *Telecommunication Technology.* 4(2): 46-48.

Wagner, A. M. "Challenge of Computer-Crime Legislation—How Should New York Respond?" *Buffalo Law Review.* 33(3): 777-814.

Waldron, Joseph, Betty Archambeault, William Archambeault, Louis Carsone, James Conser, and Carol Sutton. *Microcomputers in Criminal Justice: Current Issues and Applications.* Cincinnati: Anderson Publishing Co., 1987.

Webster, W. H. "Technology Transfer, Industrial Espionage, and Computer Crime: The FBI's Activities." *Computer Security Journal.* 3(2): 7-12.

Zedlewski, Edwin. "Computer Fraud and Abuse." Working Notes. National Institute of Justice. Washington, D.C.

Appendix A
SAMPLE APPLICATION AND AFFIDAVIT FOR SEARCH AND SEIZURE WARRANT AND OTHER LANGUAGE FOR SOME SPECIFIC PROBLEMS

DISTRICT COURT
FOR
BALTIMORE COUNTY

Application and Affidavit for Search and Seizure Warrant*

To the Honorable Judge _____ of the District Court of Maryland, for Baltimore County your affiants, DETECTIVE CALVIN L. LANE and DETECTIVE FRANK K. SIMMONS members of the Baltimore County Police Department, being duly sworn depose and say that they have reason to believe that on the premises known as 6958 Marysue DRIVE, Apt 2D, Pikesville, Maryland 21215 more particularly described as a three story brick apartment building with the numbers 6958 on the front, there is an open foyer inside with teal color doors on the apartments. Apartment 2D is located on the upper most floor. In the foyer area are mail boxes one of which is designated 2D with the name TERRAPIN on same. The apartment is located in an area known as the MILBROOK APARTMENTS.There are items subject to seizure, such as computers, keyboards, central processing units, external drives and/or internal drives, internal and/or external storage devices such as magnetic tapes and/or disks, terminals and/or video display units and /or receiving devices and peripheral equipment such as, but not limited to , printers, automatic dialers, modems, acoustical couplers and/or direct line couplers, peripheral interface boards and connecting cables and/or ribbons, customer listings, diaries, logs and other records, correspondence, journals , ledgers, memoranda, telephone and communications service billing information, computer software, programs and source documentation, computer logs, used in the obtaining, maintenance, and dissemination and/or sale of confidential information obtained from official files and computers of the MCA Telecommunications, Corporation and other evidence of the offense. Also any papers which would tent to show occupancy and/or ownership, such as utility bills, rent/lease contracts etc., for 6958 APT 2d Marysue Drive Pikesville, Maryland 21215. Further, any papers, logs, disks, files on any media which would tend to show who may be the custodian, user, owner or have interest in the above stated hardware, software or files. And, that facts tending to establish grounds for issuance of Search Warrant are set forth and the basis for the probable cause is as follows:

Your affiant DETECTIVE CALVIN L. LANE, has been a member of the Baltimore County Police Department in excess of 19 years, currently assigned to the Computer Crime Unit of the Criminal Investigation Division. During this time your affiant DETECTIVE CALVIN L. LANE has been a detective in excess of 14 years working in various specialized areas of investigation. During this fourteen year period your affiant DETECTIVE CALVIN L. LANE has been the affiant of Eighteen (18) court ordered wire taps. Also has worked on several court ordered wire taps as monitor over and above the above stated 18. Also your affiant DETECTIVE CALVIN L. LANE has established several Dialed Number Recorders as an electronic surveillance tool to monitor the activity of a telephone line. During the course of the above investigation it was required to do analysis of the information provided by the DNR paper recording tape. As a result of these investigations and DNR analysis in excess of 50 search and seizure warrants have been issued to search for various evidence. As a result of the search and seizure warrants arrests were made and convictions obtained. Your affiant Lane has also established a basis of expertise in the area of Computer crime and investigations. Your affiant has completed several college courses of study in this area to include four computer languages and a one semester course on computer crime at a local community college. A two week course conducted at the Federal Law Enforcement Training Center, Glynco, Ga., for computer crime investigations. An 80 hour instruction period conducted by the Baltimore Gas & Electric Company

*Used with permission.

in the area of computer related security. Further your affiant Lane has completed an internship with the Baltimore County Data Processing Section as a programmer. Your affiant Lane has also owned a personal computer for in excess of five years and is familiar with its use and jargon used by the personal computer community. While assigned to the Baltimore County Narcotic Section your affiant Lane was charged with the set up and design of the computer system used there, to include all aspects of its operation.

Your affiant DETECTIVE FRANK K. SIMMONS has been a member of the Baltimore County Police Department in excess of 18 years and is currently assigned to the Computer Crime unit of the criminal investigation Division. Your affiant Simmons has worked as a detective for over nine (9) years in various assignments, specializing in the area of fraud investigations. During this period your affiant Simmons has been the affiant on five previous warrants that have lead to the arrest and convictions of suspects in fraud/drug related investigations. Your affiant Simmons has investigated hundreds of felony fraud cases of all types leading to the arrest and conviction of suspects. One of these previous investigations was directly related to the theft of services from a public utility. In the area of computer related investigations your affiant has attended a two week course of study conducted at the Federal Law Enforcement Training Center, Glynco, Ga., dealing with the investigation of computer related crime. Also your affiant attended an 80 hour period of instruction on computer operations and security conducted by the Baltimore Gas & Electric Company.

Further, your affiants Lane and Simmons have as members of the Computer Crime unit executed in excess of nine search and seizure warrants. These warrants were directly related to computer seizures and their use in the violations of Maryland law. All of these cases have lead to successful prosecution of the persons involved with one pending court action.

Mr. John Jones has been an employee of the Chesapeake and Potato Telephone Company, State of Confusion, since July 9, 1970. During this period Mr. Jones has been a Service Representative, specifically working with billing IE. toll investigations and order processing. As of March 1, 1980, Mr. Jones has been assigned to the security division. Mr. Jones has received 13 weeks of Basic Programmers training and initial service representative training of that 13 weeks toll fraud investigations was includes. In the area of toll fraud the use of the Dialed Number Recorders (DNR) and the analysis of the printed data produced by the DNR was covered in detail. During Mr. Jones tenure as security investigator, he has had occasion to do in excess of 5 DNR related investigations. These investigations required the analysis of the paper DNR activity reports. Further, Mr. Jones has been awarded a B.A. in Criminology from the University of Orlando and completed a four month internship with the campus police there. Mr. Jones has also received additional college credits in the computer related studies.

Within the recent past the computer and information services industry has been plagued with a high tech intruder and thief. The tern "Hacker" is most generally used to describe this individual and can be defined as someone who makes unauthorized attempts to access a host database (computer) most generally from a remote location, often by circumventing access controls. The Hacker will use impersonation or masquerading as an authorized user to gain access to the host computer. In some instances the Hacker will in fact be an authorized user to the system and be making access attempts into unauthorized areas of the computer. The motive of the Hacker could be to browse or steal information that would offer a personal gain for the Hacker. The term Passive wire tapping could also be applied to the Hacker's activity by gaining access to the host computer the Hacker can

monitor data transmissions of records, memos or any other information being sent across communication links. Another technique used by the Hacker is scavenging of information left in unsecured areas of the computer. The computer may contain common work areas used by several people with the intent of the information being destroyed after the job has been completed. In other instances the Hacker's only intent his to cause disruptions or deny access to the rightful owners. The Hacker may insert or modify records making the owner aware of his past presence in the system.

In this present illegal scheme the Hacker is accessing the computer system of the MCA Telecommunications Corporation located at # 1 Investigation Place, Towson, Maryland in Baltimore County. The Hacker will use a computer and a device known as a modem to communicate with computer of the MCA Telecommunication Corp.. The purpose of the modem is to act as the link or interface between the two computers. The modem will translate the computer language of digital signals into aural tones that can be sent across telephone communication lines. A modem on the receiving system will then accept the aural tomes and convert them back into digital signals the computer can understand.

The host computer may, as in the case of MCA Telecommunication Corp. have a dial-in access telephone number. The access number authorizes the subscriber to communicate with the MCA computer. In the case of MCA the authorized subscriber does not need a computer to use their system in a legitimate manner. The authorized subscriber will dial the access number, enter a five digit account code and then dial the telephone number of the person to whom they wish to call. The fact that the authorized user is using a computer is transparent to them, it is only seen as a long series of numbers being dialed.

In this illegal scheme the hacker is using the computer to dial the access code for them and then sequentially trying five digit account codes with a terminating number following the code. The terminating number is another computer system. The terminating number is the telephone number of a dialup line of a computer system in this specific instance In order to instruct the Hacker's computer on what action to take given a variety of circumstances a set of coded instruction in the form of software known as a "Demon Dialer", "War Dialer" or "Hacker" is used. The reason the Hacker uses the computer is to allow for automation and record keeping to be done unattended. The Hacker's computer will then keep track of the account codes that have been tried and the ones that have been rejected as invalid codes and the ones that have been accepted as valid. If the the random code has been accepted by the MCA computer as valid the call is then forwarded to the terminating number selected by the Hacker. In this case the termination number is another computer. This number was verified by your affiant DETECTIVE FRANK K. SIMMONS as a computer. Again the reason is for automation. With a valid account code and completed call the Hacker's computer knows that it has in fact selected a valid account code. The Hacker's computer will then terminate the call to the terminating number and start the process over again. The valid code will then be recorded on the printer or to a magnetic disk file for later use. If the random code is rejected by the MCA computer the Hacker's computer will disregard the rejected account code and again starts over. Now armed with a list of valid account codes the Hacker uses these account numbers to make long distance telephone call or for communication with other computers outside his general area thus avoiding any payment to the utility for the service.

On 3/24/88 at approximately 0100 Hrs. the switch (computer) operator for the MCA Telecommunications Corporation observed what he believed to be unusual activity on their computer based telephone switching equipment. Based on his experience and computer generated reports at that time the activity was that of a "Hacker" attacking their

system. The "Hacker" continued this activity for a period of 38 hours making 3000 attempts to obtain customer billing codes. This is one attempt every 45.6 seconds. During this period there were legitimate codes compromised. Mr. Luis ABAD, MCA supervisor of the Towson switch caused a check to be made through the Chesapeake and Potato telephone company in an attempt to identify the source of the Hacking activity. It was determined that the activity was coming from 6958 Apt 2D Marysue Drive aforementioned and described.

Mr. Smith forwarded this information to the MCA Telecommunication Corp. Security Ms' Helen Brooks. Ms Brooks initiated an investigation and made a complaint to the Baltimore County Police Department and your affiants. As a part of the MCA investigative procedure Ms Brooks also contacted the Chesapeake and Potato Telephone Company, State of Maryland, Mr. John Jones. Based on agreements and contracts with MCA Telecommunication Corporation installed a Dialed Number Recorded (DNR) on telephone number (301) 555-1212 list to Ann TERRAPIN at the suspect address described above, on 3/26/88.

A dialed number recorder (DNR) is an electronic devise used to monitor line activations initiated by the opening and closing of a telephone line. When the receiver of a telephone is removed from the cradle the DNR is activated. In this case when the Hacker's computer opens the dial tone circuit via the modem. These activations are recorded on roll paper with the date and time the line was activated. The DNR will also record any numbers that are dialed when the line is open. When the line is again closed by placing the receiver on the cradle or by the modem this time is also recorded on the DNR paper. With this record of activity as recorded by the DNR an analysis can be done to determine hacking patterns and line activation indicative of calls. The DNR does not allow for oral communication to be monitored therefore completed calls are determined based on the Training, Knowledge and experience of your affiants Detectives Lane and Simmons, and Mr. John Jones of the Chesapeake and Potato Telephone Company, State of Maryland.

On 4/7/88 yours affiants Lane and Simmons went to the area of 6958 Marysue Drive Apt. 2D Pikesville, Maryland 21215. It was learned through covert interviews that a young male lived at the above address and was a student at the University of Maryland. Because of another ongoing investigation with MCA concerning the University your affiants contacted the campus police in an attempt to identify Mr. TERRAPIN. It was learned that there was a student Gregory (nmn) TERRAPIN of 6958 Marysue Drive Apt. 2D Pikesville, Maryland 21215, telephone (301) 555-1212, D.O.B. 11/12/67. Ms' Brooks of MCA advised your affiant that MCA has been experiencing a serious code abuse problem at this campus. Although Mr. TERRAPIN had not been identified, as of this date, as a targeted abuser.

As a result of the DNR being placed on the suspect line at 6958 Marysue Drive Apt. 2D Pikesville, Maryland 21215 a close monitoring of the activity could be done. The DNR showed Hacking activity directed at the MCA computer on several occasions.

3/26/88 1,302 attempts were made to obtain MCA billing codes.
3/27/88 926 attempts
3/28/88 988 attempts

During his period of Hacking activity 73 valid MCA customer codes had been compromised. These codes when used would be billed to there rightful owners. Experience has shown that these stolen codes and subsequent bills have caused their owners great anxiety. A case in point is that your affiants picked one specific code that shows abuse in this illegal scheme. A check with MCA security revealed that the customer had a maximum bill of $55.00 prior to this Hacker. The most recent bill sent out for billing period March is $461 or an increase of $406.00 over the customer's past highest bill.

This Hacking activity has been on going with thousands of attempts to steal codes. Also these stolen codes have been used, which are billed to their rightful owners. The most recent DNR tape being analyzed was dated up to and including 4/13/88. On 4/13/88 Hacking activity began at 0025 Hrs. to 0625 Hrs. six hours. It is the belief of your affiants based on past experience and the pattern of activity date in this specific illegal scheme, that it will continue until action is taken by law enforcement.

Therefore, your affiants believe based on their Training, Knowledge and Experience that evidence of theft, unlawful access to a computer and a device to avoid telephone charges is located on the premises known as 6958 Marysue DRIVE, Apt 2D, Pikesville, Maryland 21215 described above. Past experience has proven that "Hackers" will maintain records of their activity for long periods of time. It is not unusual for these records to be kept for eight to ten months. This information is traded amongst "Hackers". Information is the "coin of the realm" to be exchanged between hackers. The hacker with the most information is held in esteem. Codes tried and failed are also valuable so as not to repeat past mistakes.

Therefore, your affiants pray that a Search and Seizure warrant be issued, authorizing that any Police Officer with authority in this jurisdiction, with the necessary and proper assistance to enter and search the aforementioned and described location and to search for and seize all contraband, evidence, fruits of the crime, and instrumentalities of the crime, which are subject to seizure and are in violation of, or evidence of, the violation of, the Laws of Maryland pertaining to illegal Access to a Computer Article 27 Section 146, Theft Article 27 Section 340-342 and Device to avoid Telephone Charges Article 27 Section 557A.

Signature of Affiant

Signature of Affiant

SWORN to before Me and subscribed to in my presence this day of 1988.

JUDGE

SAMPLE AFFIDAVIT LANGUAGE FOR PARTICULAR PROBLEMS:

1. Justification for seizing hardware, etc. (where appropriate):

Affiant interviewed _____, employed as a _____ in the _____ office. _____ informed affiant that in connection with his employment, he uses computer systems as well as conducting computer-related investigations. In the past two years, _____ has supervised or participated in several executions of search warrants for computer-stored records and evidence. _____ informed affiant that conducting a search of a computer system, documenting the search, and making evidentiary and discovery copies is a lengthy process. It is necessary to determine that no security devices are in place which could cause the destruction of evidence during the search; in some cases it is impossible even to conduct the search without expert technical assistance. Since computer evidence is extremely vulnerable to tampering or to destruction through error, electrical outages, and other causes, removal of the system from the premises will assist in retrieving the records authorized to be seized, while avoiding accidental destruction or deliberate alteration of the records. It would be extremely difficult to secure the system on the premises during the entire period of the search.

_____ also stated that whether records are stored on floppy disks or on a hard drive, even when they purportedly have been erased or deleted, they may still be retrievable. _____ is familiar with the methods of restoring "lost" data commonly employed by computer users, and has used those methods himself. _____ has also obtained the assistance of a computer expert in several cases, in order to obtain the contents of computer-stored evidence, where normal methods were unsuccessful. He stated that should such data retrieval be necessary, it is time-consuming, and would add to the difficulty of securing the system on the premises during the search.

_____ stated that the accompanying software must also be seized, since it would be impossible without examination to determine that it is standard, commercially available software: it is necessary to have the software used to create data files and records in order to read the files and records. In addition, without examination, it is impossible to determine that the diskette purporting to contain a standard commercially available software program has not been used to store records instead.

_____ informed affiant that the system documentation, instruction manuals, and software manuals are also necessary to properly operate that specific system in order to accurately obtain the records authorized to be seized.

2. Dialled number recorder (DNR)/pen register:

A dialled number recorder captures the electronic impulses travelling over a telephone line as the numbers on a telephone are dialled or pushed. The device records the numbers dialled or pushed on a paper tape (NB: not always! newer ones may include magnetic-media storage) for review, but does not record the content of the communication. A dialled number recorder, in addition, records any transmission of the special signalling tones which are used to control communications networks and their associated automatic billing systems. (see below)

3. Tone generator -- "blue box" or "blue computer":

_____ from the _____ Telephone Company advised that special signalling tones are used to control communications networks and their associated automatic billing systems. The special signalling tones can be generated by an electronic tone-generating device known as a "blue box", or by a personal computer and software programs which enable the computer to generate the tone signal through a communications device (a modem or accoustic coupler) connecting the computer to the telephone line. In his past investigations, _____ has frequently found that persons stealing communications services have possessed a personal computer and the necessary software which would allow them to manipulate communications networks by means of the special signalling tones.

4. Packet-switched networks:

_____, an employee of the ____Net informed affiant that the ____Net is a packet-switching common carrier providing facilities for the transmission of data, rather than voice communications, for its subscribers. ____Net maintains high-speed communications lines which are used to transmit "packets" of data throughout the United States. At various places on the network, ____Net maintains communications handling devices (or switches), some of which are accessed by telephones using commercial telephone lines. A subscriber may gain access to the network by dialling its local telephone number, connecting the subscriber to the switch. When the connection is complete, the subscriber hears an audible tone and connects his telephone receiver to his modem or accoustic coupler, connected to his computer. (This step is omitted with an automatic modem connecting the computer directly with the telephone line.)

Once the communication link has been established, the caller must enter certain fixed-format information which identifies the "address" of the subscriber computer system with which he wishes to communicate. The caller must then enter certain fixed-format information, including a password and/or user identification number, which are known only to authorized users and are registered in the computer system.

A similar communications network operating in Canada is ____Pac; communications between American ____Net and Canadian ____Pac subscribers can be routed through the "Gateway", a communications facility in Canada, allowing subscribers of each network to send communications to subscribers of the other.

5. "Voice-Mail" Systems:

The _____ voice-mail system allows authorized _____ employees to obtain a "voice mailbox" which is capable of performing several functions. Among these are the ability to receive and store messages from callers, to send messages to other boxes on the system, and to send messages to a pre-selected group of boxes. These functions are achieved by pushing the appropriate numerical commands on a telephone keypad for the desired function.

To leave a message, the caller dials the company's "800" telephone number, and hears a greeting identifying the system as the _____ voice-message system, along with instructions for leaving a message. The caller can exercise several options, one of which is to leave a message after the tone. In this respect, the voice-mail system operates much like a telephone answering machine. Rather than being recorded on audio tape, however, the message is stored in digitized form by the computer system. The entire voice-message system is actually a computer system accessible through the company's telephone lines. The dictated messages are stored on large-capacity computer disks.

An outside caller needs to know only the assigned box number (the same as the telephone extension number) in order to leave a message for a _____ employee. In order to retrieve the messages or to delete them from the system, however, the person to whom the box is assigned must know both the box number and a confidential password -- the password ensures privacy of the communications, by acting as a "key" to "unlock" the box and reveal its contents. The employee to whom the box has been assigned also has the ability to change his password, thereby preventing access to the box contents by anyone who may have learned his password.

Since _____, 198_, authorized users of the _____ voice-mail system have been reporting abuse of the system, including the "taking over" of numerous boxes by unknown persons who somehow obtained the passwords, gained access to the boxes, then changed the passwords to deny access to the assigned users. _____ also reported a significant increase in use of the system, and in incoming "800"-line calls, during this period. While _____ does not yet know the full extent of its losses, the company pays the charges for calls made on their "800" line, and the unauthorized users have interrupted service to _____ employees and customers. The unauthorized users have occupied a significant portion of the system's disk capacity, necessitating the purchase and installation of an additional disk, at a cost of $_____, in order to avoid further damage to the company's communication system.

Appendix B

SAMPLE SEARCH AND SEIZURE WARRANT AND OTHER RELEVANT MATERIAL

DISTRICT COURT
FOR
BALTIMORE COUNTY

Search and Seizure Warrant*

To: Any Police Officer of Baltimore County

Affidavit having been made before me by Detective Calvin Lane and Detective Frank Simmons, members of the Baltimore County Police Department, that they have reason to believe that on the premises known as 6958 MARYSUE DRIVE, Apt 2D, Pikesville, Maryland 21215 more particularly described as a three story brick apartment building with the numbers 6958 on the front, there is an open foyer inside with teal color doors on the apartments. Apartment 2D is located on the upper most floor. In the foyer area are mail boxes one of which is designated 2D with the name TERRAPIN on same. The apartment is located in an area known as the MILBROOK APARTMENTS.

In the County of Baltimore, there is now property subject to seizure, such as computers, keyboards, central processing units, external and/or internal drives, internal and/or external storage devices such as magnetic tapes and/or disks, terminals and/or video display units and/or receiving devices and peripheral equipment such as, but not limited to, printers, automatic dialers, modems, acoustic couplers and or direct line couplers, peripheral interface boards and connecting cables and or ribbons, diaries, logs, and other records, correspondence, journals, ledgers memoranda, computer software, programs and source documentation, computer logs, magnetic audio tapes and recorders used in the obtaining, maintenance, and or dissemination of information obtained from the official files and computers of the MCI Telecommunications Inc. and other evidence of the offense. Also, any papers which would tend to show occupancy or ownership for the residence of,6958 MARYSUE DRIVE, Apt 2D, Pikesville, Maryland 21215 such as utility bills, rent and or lease agreements etc. Further any papers, logs, disks or files on any media which would tend to show who may be the custodian, user, owner or interest in. the above stated hardware, software or files, which are in violation of, or evidence of the violation of, the Laws of Maryland pertaining to Article 27 Section 340, theft, Article 27 Section 146, Unauthorized access to a computer, Article 27 Section 557 A, Device to avoid telephone charges, and I am satisfied that there is probable cause to believe that the property so described is on the premises above described and that the grounds for the issuance of the search warrant exists, being those grounds as stated on the application and affidavit attached hereto and incorporated herein by reference.

You are, therefore, hereby commanded with the necessary and proper assistance, to search forthwith the premises herein above described for the property herein above specified, executing this warrant and making the search; and if the property be found there, to seize it; leaving a copy of said warrant, Application/Affidavit therefore with an inventory of the property seized and returning a copy of said warrant, Application/Affidavit and inventory, if any to me within ten (10) days after the execution of this warrant; or if not served, to return this warrant and Application/Affidavit to me within five (5) working days after its expiration, as required by law.

Dated this day of , 1988

Signed ----------
Judge

*Used with permission.

EXCERPTS FROM COMPUTER SEARCH WARRANTS

ITEMS TO BE SEARCHED FOR AND SEIZED:

1. Electronic data processing and storage devices, computers and computer systems including central processing units; internal and peripheral storage devices such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices or other memory storage devices; peripheral input/output devices such as keyboards, printers, video display monitors, optical readers, and related communications devices such as modems; together with system documentation, operating logs and documentation, software and instruction manuals.

Note: this type of language applies to the situation in which the presence of a personal or small business computer is suspected (a large drug operation), or probable (a computer hacker), but where it has been impossible to determine in advance what kind of system it is. Ideally, investigation prior to execution of the warrant has produced specific information about the system, and those specifics should then be included in the description of items to be seized.

2. [Description of specific records to be seized]
All of the above records, whether stored on paper, on magnetic media such as tape, cassette, disk, diskette or on memory storage devices such as optical disks, programmable instruments such as telephones, "electronic address books", calculators, or any other storage media, together with indicia of use, ownership, possession, or control of such records.

Note: if the search warrant is properly specific as to the nature and content of records to be seized, the form in which the record is found should be irrelevant. However, to avoid challenges to the seizure of computer diskettes, etc. not mentioned in a traditional "books and records" warrant, some language such as this should be included in situations in which it is not absolutely known that all the records sought are on paper. Of course, the search team can always obtain a supplemental warrant if there is any doubt that records found in unexpected "hardware" form, such as a programmable electronic telephone directory, are authorized to be seized.

Appendix C
PROFESSIONAL ASSOCIATIONS PROVIDING SUPPORT TO THE INVESTIGATION AND PROSECUTION OF COMPUTER-RELATED CRIME

PUBLIC SECTOR ASSOCIATIONS

FEDERAL COMPUTER INVESTIGATIONS COMMITTEE (FCIC)
c/o U.S. Secret Service Fraud Division, Room 942
1800 G Street, N.W. Phone: (202) 535-5850
Washington, D.C. 20223 Steve Purdy

This committee has been in existence for about three years. It is comprised of representatives from federal military and civilian law enforcement agencies. The organization meets three times a year for the purpose of enhancing techniques to investigate computer-related crimes. The committee strives to develop universal guidelines for these types of investigations. Membership is diverse (U.S. Secret Service, IRS, FBI, Department of Defense, CID, AFOSI, NIS, Department of Labor, and others), which contributes to a broad-based forum for developing techniques and guidelines. Participating agencies and private industry provide specialized training for members. Non-voting members from state and local governments also participate in Association meetings.

HIGH TECH CRIME INVESTIGATOR'S ASSOCIATION (HTCIA)
c/o L.A. County Sheriff's Dept. (Forgery/Fraud Detail)
11515 South Colima Road, Rm. M104 Phone: (213) 946-7212
Whittier, California 90604 Jim Black—President

Members include federal, state and local law enforcement personnel as well as security managers from private industry. The association brings together private industry and law enforcement officials in order to communicate and educate each other about computer-related crimes.

COLORADO ASSOCIATION OF COMPUTER CRIME INVESTIGATORS
c/o Larry Scheideman
Lakewood Police Dept.
Lakewood, Colorado 80226-3105 Phone: (303) 987-7370

Founded: 1986. A professional association including federal, state, and local law enforcement personnel and those persons from the private sector concerned with computer crime. The association assists law enforcement agencies with resource allocation and intelligence/investigation of computer-related crimes. The Association also provides training on an individual basis.

LAW ENFORCEMENT ELECTRONIC TECHNOLOGY ASSISTANCE COMMITTEE (LEETAC)

Office of the State Attorney
700 South Park Avenue — Phone: (407) 269-8112
Titusville, Florida 32781 — Jim Graham

The organization is comprised of 10 prosecutors from the State's Attorney's office, 13 officers representing each municipality in the county, 2 representatives from the sheriff's department, and Nassau. They provide technical expertise to law enforcement regarding computer crimes.

INTERNATIONAL ASSOCIATION OF CREDIT CARD INVESTIGATORS (IACCI)

Phone: (415) 897-8800
1620 Grant Avenue — D.D. Drummond
Norato, California 94945 — Executive Director

Founded: 1968. Members: 2700. Special agents, investigators, and investigation supervisors who investigate criminal violations of credit card laws and prosecute offenders; law enforcement officers, prosecutors or related officials who investigate, apprehend and prosecute credit card offenders; employees of card issuing institutions who are responsible for credit card security and investigations. The Association's objective is to aid in the establishment of effective credit card security programs; to suppress fraudulent use of credit cards; and to detect and proceed with the apprehension of credit card thieves. Provides workshops, training conferences and seminars to acquaint law enforcement and the membership with technological advances in the industry.

ECONOMIC CRIME INVESTIGATOR'S ASSOCIATION (ECIA)

Glendale Police Department
7119 N. 57 Drive — Phone: (602) 931-5511
Glendale, Arizona 85301 — Wayne Cerow

Members include law enforcement and regulatory personnel. The Association focuses on economic crime, including computer-related crimes. The Association holds a yearly training seminar in order to exchange information, ideas and data on new technological advances.

PRIVATE ASSOCIATIONS

INSTITUTE OF INTERNAL AUDITORS (IIA)
249 Maitland Avenue
Altamonte Springs, Florida 32701 Phone: (407) 830-7600

Founded: 1941. Members 30,000. Staff: 74: Local Group: 183 Professional organization of internal auditors, comptrollers, accountants, educators, and computer specialists. IIA holds an annual conference which offers training and education on detection of computer-related crimes. IIA does research in the areas of whistle blowing, fraud, ethics, and technology. Individual members have assisted both state/local police with investigations involving computer-related crime.

COMPUTER LAW ASSOCIATION, INC. Phone: (703) 560-7747
8303 Arlington Boulevard, Suite 210 Barbara Fieser
Fairfax, Virginia 22031 (Executive Director)

Founded: 1973. Members 1200. Lawyers, law students, and others interested in legal problems related to computer communications technology. The Association sponsors continuing legal education on computer law. CLA also publishes a reference manual which lists organizations involved with computer law.

COMMUNICATIONS FRAUD CONTROL ASSOCIATION (CFCA)
Phone: (703) 848-9760
P.O. Box 23891 Rami Abuhamdeh
Washington, D.C. 20026 (Executive Director)

A security organization involved in investigations of telecommunications fraud. Membership includes: (a) individual and corporate, (b) associate individual, and (c) vendor.

NATIONAL CENTER FOR COMPUTER CRIME DATA (NCCD)
Phone: (213) 874-8233
2700 North Cahuenga Boulevard Jay BloomBecker
Los Angeles, California 90068 (Director)

Founded: 1978. The Center disseminates data and documents in order to facilitate the prevention, investigation and prosecution of computer crime. The Center sponsors speakers and seminars. The Center also is involved in conducting research and compiling statistics.

MIS TRAINING INSTITUTE
Information Security Division
498 Concord Street
Framingham, Massachusetts 01701 Phone: (508) 879-7999

Information security seminars for information security professionals, EDP auditors, and data processing management. The institute provides both training and consulting services, and has assisted local police in investigations of computer-related crimes.

COMPUTER VIRUS INDUSTRY ASSOCIATION Phone: (408) 988-3832
4423 Cheeney Street John McAfee
Santa Clara, California 95054 Executive Director

Founded 1987. Objective is to help identify, and cure computer viruses. The association has worked with state and local law enforcement agencies in the investigation and detection of computer and computer-related crimes.

INFORMATION SYSTEMS SECURITY ASSOCIATION (ISSA)
P.O. Box 71926 Phone: (714) 863-5583
Los Angeles, California 90071 Carl B. Jackson

Founded: 1982. Members: 300. Computer security practioners whose primary responsibility is to ensure protection of information assets on a hands-on basis. Members include banking, retail, insurance, aerospace, and publishing industries. The association's objectives is to increase knowledge about information security. ISSA sponsors educational programs, research, discussion, and dissemination of information. The Association has regional and state chapters.

SRI INTERNATIONAL
Information Security Program
333 Ravenswood Avenue Phone: (415) 859-2378
Menlo Park, California 94025 Donn B. Parker

Founded: 1947. A staff of senior consultants and computer scientists perform research on computer crime and security and provide consulting to private and government clients worldwide. A case file of over 2,500 computer abuses since 1958 has been collected and analyzed. It is available for use by criminal justice agencies and students free of charage. An electronic bulletin board, Risks Forum, is operated and sponsored by the Association for Computing Machinery to collect and disseminate information about risks in using computers.

Appendix D

LAW SCHOOLS OFFERING COURSES IN COMPUTER LAW *

* Schools responding to a survey by the Computer Law Association, Inc., 703-560-7747. Information compiled as of October 1988.

1. The University of Akron
School of Law
302 East Buchtel Avenue
Akron, OH 44325
216-375-7331

2. The American University
Washington College of Law
4400 Massachusetts Avenue, N.W.
Washington, D.C. 20016
202-885-2606

3. Arizona State University
College of Law
Tempe, AZ 85287
602-965-6181

4. Boston College
Law School
885 Centre Street
Newton Centre, MA 02159
617-552-4350

5. Campbell University
School of Law
P.O. Box 158
Buies Creek, NC 27506
919-893-4111

6. Capital University
Law School
665 South High Street
Columbus, OH 43215
614-445-8836

7. Cleveland State University
Cleveland-Marshall College of Law
Cleveland, OH 44115
216-687-2344

8. Columbia University
School of Law
435 West 116th Street
New York, NY 10027
212-280-2670

9. Thomas M. Cooley Law School
217 South Capitol Avenue
P.O. Box 13038
Lansing, MI 48901
517-371-5140

10. Cornell University
Cornell Law School
Myron Taylor Hall
Ithaca, NY 14853
607-256-5141

11. University of Denver
College of Law
Montview and Quebec Streets
Denver, CO 80220
303-871-6000

12. Detroit College of Law
130 East Elizabeth Street
Detroit, MI 48201
313-965-0150

13. The Dickinson School of Law
150 South College
Carlisle, PA 17013
717-243-4611

14. Drake University
Law School
27th and Carpenter Streets
Des Moines, IA 50311
515-271-2824

15. Emory University
School of Law
Gambrell Hall
Atlanta, GA 30322
404-727-6509

16. University of Florida
College of Law
Holland Law Building
Gainesville, FL 32611
904-392-2087

17. Fordham University
School of Law
140 West 62nd Street
New York, NY 10023
212-841-5191
201-871-3712

18. Franklin Pierce Law Center
2 White Street
Concord, NH 03301
603-228-1541

19. Georgia State University
University Plaza
Atlanta, GA 30303-3092
404-651-2087

20. Georgetown University
Law Center
600 New Jersey Avenue, N.W.
Washington, D.C. 20010
202-624-8320

21. Golden Gate University
School of Law
536 Mission Street
San Francisco, CA 94105
415-442-7250

22. Hamline University
School of Law
1536 Hewitt Avenue
St. Paul, MN 55104
612-641-2400

23. Harvard University
Harvard Law School
Cambridge, MA 02138
617-495-3109

24. University of Hawaii at Monoa
William S. Richardson
School of Law
2515 Dole Street
Honolulu, HI 96822
808-948-7966

25. University of Houston
Law Center
4800 Calhoun
Houston, TX 77004
713-749-4816

26. Illinois Institute of Technology
Chicago-Kent College of Law
77 South Wacker Drive
Chicago, IL 60606
312-567-5000

27. John Marshall Law School
315 South Plymouth Court
Chicago, IL 60604
312-987-1445

28. University of Louisville
School of Law
Belknap Campus
2301 South Third Street
Louisville, KY 40292
502-588-6364

29. Loyola Marymount University
Loyola Law School
1441 West Olympic Boulevard
Los Angeles, CA 90015-3980
213-736-1000

30. University of Maryland
School of Law
500 West Baltimore Street
Baltimore, MD 21201
301-528-7214

31. Massachusetts Institute
of Technology
77 Massachusetts Avenue
Cambridge, MA 02139
617-253-4932

32. University of Minnesota
Law School
229 19th Avenue South
Minneapolis, MN 55455
612-625-2371

33. The University of Mississippi
School of Law
University, MS 38677
601-232-7361

34. University of Montana
School of Law
Missoula, MT 59812
406-243-4311

35. University of New Mexico
School of Law
1117 Standord Drive, N.E.
Albuquerque, NM 87131
505-277-2146

36. New York Law School
57 Worth Street
New York, NY 10013
212-431-2888

37. University of North Carolina
at Chapel Hill
School of Law
Van Hecke-Wettach Hall, 064-A
Chapel Hill, NC 27514
919-962-5106

38. University of North Dakota
School of Law
University Station
Grand Forks, ND 58202
701-777-2104

39. Northwestern University
School of Law
357 East Chicago Avenue
Chicago, IL 60611
312-346-4585

40. The University of Oklahoma
College of Law
300 Timberdell Road
Norman, OK 73019
405-325-6909

41. University of Oregon
School of Law
Eugene, OR 97403
503-686-3846

42. Oxford University
University Offices
Wellington Square
Oxford, OX1 2JP
England
0865 56747

43. Pepperdine University
School of Law
24255 Pacific Coast Highway
Malibu, CA 90265
213-456-4611

44. University of Pittsburgh
School of Law
3900 Forbes Avenue
Pittsburgh, PA 15260
412-624-6200

45. Rutgers University
School of Law
5th and Penn Streets
Camden, NJ 08182

46. University of Santa Clara
School of Law
Santa Clara, CA 95053
408-984-4361

47. The University of Southampton
Faculty of Law
Southampton, UK
SO9 5NH 0101(703)
559122 Ext. 3404/3526

48. Southern Illinois University
School of Law
Carbondale, IL 62901
618-536-7711

49. The University of Tennessee
College of Law
1505 West Cumberland Avenue
Knoxville, TN 37996-1800
615-974-4131

50. University of Toronto
Faculty of Law
Queen's Park
Toronto, Ontario
Canada
416-362-1812

51. The University of Tulsa
College of Law
3120 East Fourth Place
Tulsa, OK 74104
918-592-6000 C:2709

52. The University of Utah
College of Law
Salt Lake City, UT 84112
801-581-6833

53. Villanova University
School of Law
Garey Hall
Villanova, PA 19085
215-645-7010

54. University of Washington
School of Law
Condon Hall, JB-20
Seattle, WA 98195
206-543-4550

55. University of Waterloo
Department of Computer Science
Waterloo, Ontario
Canada N2L 3G1
519-885-1211

56. University of Wyoming
College of Law
Box 30353
University Station
Laramie, WY 82071
307-766-6416

57. William Mitchell College of Law
875 Summit Avenue
St. Paul, MN 55105
612-227-9171

Appendix E
COMPUTER CRIME STATUTES

Alabama	Ala. Code 13A-8-101
Alaska	Alas. Stat. sec. 11.46.740 and 11.81.900(b)(44) Alas. Stat. sec. 11.46.200(a)
Arizona	Ariz. Rev. Stat. sec. 13-2301E. Also, 13-2316
Arkansas	Ark. Stat. sec. 5-41-102 - 5-41-106
California	Cal. Penal Code sec. 502
Colorado	Colo. Rev. Stat. sec. 18-5.5-101
Connecticut	Conn. Gen. Stat. Ann. sec. 53a-250
Delaware	Del. Code tit. 11, sec. 931 to 939
Florida	Fla. Stat. Ann. sec. 815.01
Georgia	Ga. Code Ann. sec. 16-9-90
Hawaii	Haw. Rev. Stat. 708-890
Idaho	Session Laws of Idaho 1984, ch. 68, p. 129, adding Idaho Code sec. 18-2201
Illinois	Ill. Stat. Ann. ch. 38, sec. 16D-1 - 16D-7
Indiana	IC 35-43-1-4, IC 35-43-2-3
Iowa	Iowa Code Ann. sec. 716A
Kansas	Kans. Stat. sec. 21-3755
Kentucky	Ch. 210, Acts of 1984, adding Ky Rev. Stat. sec. 434.840
Louisiana	La. Rev. Sat. 14:73.1 through 5
Maine	Me. Rev. Stat. Ann. tit. 17-A sec. 357 (1964)
Maryland	Md. Ann. Code Art. 27, sec. 146
Massachusetts	Mass. Gen. Laws Ann. ch. 266, sec. 30(2)
Michigan	Mich. Comp. Laws Ann. sec. 752.791
Minnesota	Minn. Stat. Ann. sec. 609.87
Mississippi	Miss. Code Ann. sec. 97-45-1
Missouri	Mo. Ann. Stat. sec. 569.093
Montana	Mont. Code Ann. 45-6-310
Nebraska	Neb. Rev. Stat. sec. 28-1343
Nevada	Nev. Rev. Stat. sec. 205.473
New Hampshire	N.H. Rev. Stat. Ann. sec. 638:16
New Jersey	NJ. Rev. Stat. sec. 2A:38A-1 and NJ. Rev. Stat. sec. 2C:20-23
New Mexico	Computer Crimes Act of 1979. N.M. Stat. Ann. sec. 30-16A-1
New York	N.Y. Penal Law Art. 156
North Carolina	N.C. Gen. Sat. 14-453
North Dakota	N.D. Cent. Code sec. 12.1-06.1-08
Ohio	Ohio Rev. Code Ann. sec. 2901.01 and 2913.01
Oklahoma	Okla. Stat. Ann. tit. 21, sec. 1952-1956
Oregon	Or. Rev. Stat. 164.377
Pennsylvania	Pa. Stat. Ann. tit. 18, sec. 3933

Rhode Island	R.I. Gen. Laws sec. 11-52-1
South Carolina	S.C. Code sec. 16-16-10
South Dakota	S.D. Codified Laws Ann. sec. 43-43B-1
Tennessee	Tenn. Code Ann. sec. 39-3-1401
Texas	Tex. Penal Code sec. 33.01-33.05
Utah	Utah Code Ann. sec. 76-6-701
Virginia	Va. Code Ann. sec. 18.2-152.1
Washington	Wash. Rev. Code Ann. sec. 9A.48.100
Wisconsin	Wisc. Stat. Ann. sec. 943.70
Wyoming	Wyo. Stat. sec. 6-3-501 through 504
Federal law	18 U.S.C. 1030, as amended by PL99-474 in 1986 and 18 U.S.C. 1029

Appendix F
U.S. SECRET SERVICE FIELD OFFICES*

* RA = Resident Agent
D = Domicile

City	Telephone
Albany, GA (RA)	912-430-8442
Albany, NY (RA)	518-472-2884
Albuquerque	505-766-3336
Anchorage (RA)	907-271-5148
Atlanta	404-331-6111
Atlantic City (RA)	609-347-0772
Augusta, GA (D)	404-722-7894
Austin	512-482-5103
Bakersfield, CA (D)	805-861-4112
Baltimore	301-962-2200
Baton Rouge (RA)	504-389-0763
Beaumont, TX (D)	409-866-0776
Birmingham	205-731-1144
Bismarck (RA)	701-255-3284
Boise (RA)	208-334-1403
Boston	617-565-5640
Buffalo	716-846-4401
Canton (RA)	216-489-4400
Charleston, SC (RA)	803-724-4691
Charleston, WV	304-347-5188
Charlotte	704-523-9583
Chattanooga (RA)	615-266-4014
Cheyenne (RA)	307-772-2380
Chicago	312-353-5431
Cincinnati	513-684-3585
Cleveland	216-522-4365
Colorado Springs (D)	303-594-4910
Columbia	803-765-5446
Columbus	614-469-7370
Concord (RA)	603-225-1615
Corpus Christi (RA)	512-888-3401
Dallas	214-767-8021
Dayton (RA)	513-222-2013
Denver	303-844-3027
Des Moines (RA)	515-284-4565
Detroit	313-226-6400
El Paso	915-541-7546
Flint, MI (D)	313-234-7223
Ft. Myers, FL (D)	813-337-3966
Fort Smith, AR (D)	501-452-4482
Fort Worth (RA)	817-334-2015

City	Telephone
Frederick, MD (D)	301-293-1958
Fresno (RA)	209-487-5204
Grand Rapids	616-456-2276
Great Falls	406-452-8515
Greenville (RA)	803-233-1490
Harlingen, TX (D)	512-428-9311
Harrisburg (RA)	717-782-4811
Honolulu	808-541-1912
Houston	713-229-2755
Indianapoliis	317-269-6444
Jackson	601-965-4436
Jacksonville	904-724-4530
Kansas City	816-426-5022
Knoxville (RA)	615-673-4527
Las Vegas (RA)	702-388-6446
Lexington (RA)	606-233-2453
Little Rock	501-378-6241
London (RA)	499-9000x2394
Los Angeles	213-894-4830
Louisville	502-582-5171
Lubbock (RA)	806-743-7347
Madison (RA)	608-264-5191
Melville (RA)	516-249-0404
Memphis	901-521-3568
Miami	305-591-3660
Midland, TX (D)	915-683-6923
Milwaukee	414-291-3587
Minneapolis	612-348-1800
Mobile	205-690-2851
Montgomery (RA)	205-832-7601
Nashville	615-251-5841
Newark	201-645-2334
New Haven	203-865-2449
New Orleans	504-589-4041
New York	212-466-4400x2184
Norfolk	804-441-3200
Northern VA (D)	703-378-1979
Oklahoma City	405-231-4476
Omaha	402-221-4671
Orlando (RA)	305-648-6333
Oxford, MS (D)	601-236-1563
Panama City, FL (D)	904-265-5323
Paris	4296-1202 x2306

City	Telephone
Philadelphia	215-597-0600
Phoenix	602-261-3556
Pittsburgh	412-644-3384
Portland, ME (RA)	207-780-3493
Portland, OR	503-221-2162
Providence	401-331-6456
Raleigh (RA)	919-790-2834
Reno (RA)	702-784-5354
Richmond	804-771-2274
Riverside (RA)	714-351-6781
Roanoke (RA)	703-982-6208
Rochester (RA)	716-263-6830
Rome	46741 x2694
Sacramento	916-551-2802
Saginaw (RA)	313-234-7223
St. Louis	314-425-4238
Salt Lake City	801-524-5910
San Antonio	512-229-6175
San Diego	619-557-5640
San Francisco	415-556-6800
San Jose (RA)	408-291-7233
San Juan	809-753-4539
Santa Barbara (RA)	805-963-9391
Savannah (RA)	912-944-4401
Scranton (RA)	717-346-5781
Seattle	206-442-5495
Shreveport (RA)	318-226-5299
Sioux Falls (RA)	605-331-4565
Spokane	509-456-2532
Springfield, IL	217-492-4033
Springfield, MO (RA)	417-864-8340
Syracuse	315-423-5338
Tallahassee, FL (D)	904-877-0855
Tampa	813-228-2636
Toledo	419-259-6434
Tucson (RA)	602-629-6823
Tulsa (RA)	918-581-7272
Tyler (RA)	214-534-2933
Waco, TX (D)	817-848-4946
Washington	202-634-5100
West Palm Beach (RA)	407-659-0184
White Plains (RA)	914-682-8181

City	Telephone
Wichita (RA)	316-267-1452
Wilmington, DE (RA)	302-573-6188
Wilmington, NC (RA)	919-343-4411
Youngstown, OH (D)	216-726-0180

APPENDIX G
FEDERAL BUREAU OF INVESTIGATION FIELD OFFICES

City	Address	Telephone
Albany, New York 12201-1219	5th Floor, 445 Broadway, USPO & CH	518 465-7551
Albuquerque, New Mexico 87102	301 Grand Avenue, N.E.	505 247-1555
Alexandria, Virginia 22314	Room 500, 300 North Lee Street	703 683-2680
Anchorage, Alaska 99513	Fed. Bldg., Room E-222, 701 C Street	907 276-4441
Atlanta, Georgia 30302	275 Peachtree Street, N.E., 10th Floor	404 521-3900
Baltimore, Maryland 21207	7142 Ambassador Road	301 265-8080
Birmingham, Alabama 35203	Room 1400 -2121 Building	205 252-7705
Boston, Massachusetts 02203	John F. Kennedy Federal Office Building	617 742-5533
Buffalo, New York 14202	Room 1400, 111 West Huron Street	716 856-7800
Butte, Montana 59702	115 U.S. Court House and Federal Bldg.	406 782-2304
Charlotte, North Carolina 28217	6010 Kenley Lane	704 529-1030
Chicago, Illinois 60604	Room 905, Everett M. Dirksen Bldg.	312 431-1333
Cincinnati, Ohio 45202	Room 9023, 550 Main Street	513 421-4310
Cleveland, Ohio 44199	3005 Federal Office Building	216 522-1400
Columbia, South Carolina 29201	Suite 1357, 1835 Assembly Street	803 254-3011
Dallas, Texas 75202	Suite 300, 1801 North Lamar Street	214 720-2200
Denver, Colorado 80202	Room 1823, Federal Office Building	303 629-7171
Detroit, Michigan 48226	P. V. McNamara Bldg., 477 Michigan Ave.	313 965-2323
El Paso, Texas 79901	Suite C-600, 700 E. San Antonio Avenue	915 533-7451
Honolulu, Hawaii 96850	Room 4307, Kalanianaole Federal Bldg., 300 Ala Moana Boulevard	808 521-1411
Houston, Texas 77002	6015 Federal Bldg. and U.S. Court House	713 224-1511
Indianapolis, Indiana 46204	Rm. 679, 575 North Pennsylvania Street	317 639-3301
Jackson, Mississippi 39269	Suite 1553, Fed. Bldg., 100 W. Capitol St.	601 948-5000
Jacksonville, Florida 32211	Oaks V, 4th Fl., 7820 Arlington Expwy.	904 721-1211
Kansas City, Missouri 64106	Room 300, U.S. Court House	816 221-6100
Knoxville, Tennessee 37919	Room 800, 1111 Northshore Drive	615 588-8571
Las Vegas, Nevada 89104	700 E. Charleston Boulevard	702 385-1281
Little Rock, Arkansas 72201	Suite 200, 10825 Financial Centre Pkwy.	501 221-9100
Los Angeles, California 90024	11000 Wilshire Boulevard	213 477-6565
Louisville, Kentucky 40202	Room 502, FOB, 600 Federal Place	502 583-3941
Memphis, Tennessee 38103	841 Clifford Davis Federal Building	901 525-7373
Miami, Florida 33169	16320 2nd Ave., N.W., N. Miami Beach	305 944-9101
Milwaukee, Wisconsin 53202	Rm. 700, Federal Bldg. & U.S. Court House	414 276-4684
Minneapolis, Minnesota 55401	392 Federal Building	612 339-7861
Mobile, Alabama 36602	One St. Louis Centre	205 438-3674
Newark, New Jersey 07102	Gateway 1, Market Street	201 622-5613
New Haven, Connecticut 06510	Federal Building, 150 Court Street	203 777-6311
New Orleans, Louisiana 70113	Suite 2200, 1250 Poydras Street	504 522-4671
New York, New York 10278	26 Federal Plaza	212 553-2700
Norfolk, Virginia 23510	Room 839, 200 Granby Street	804 623-3111
Oklahoma City, Oklahoma 73118	Suite 1600, 50 Penn Place	405 842-7471
Omaha, Nebraska 68102	Room 7401, Federal Bldg., USPO and CH, 215 North 17th Street	402 348-1210
Philadelphia, Pennsylvania 19106-1611	8th Floor, FOB, 600 Arch Street	215 829-2700
Phoenix, Arizona 85012	Suite 400, 201 East Indianola	602 279-5511
Pittsburgh, Pennsylvania 15222	Room 1300, Federal Office Building	412 471-2000
Portland, Oregon 97201	Crown Plaza Building	503 224-4181
Richmond, Virginia 23220	200 West Grace Street	804 644-2631
Sacramento, California 95825	Federal Building, 2800 Cottage Way	916 481-9110

City	Address	Telephone
St. Louis, Missouri 63103	2704 Federal Building	314 241-5357
Salt Lake City, Utah 84138	3203 Federal Building	801 355-7521
San Antonio, Texas 78205	Room 433, Old P.O. Bldg., 615 E. Houston	512 225-6741
San Diego, California 92188	Room 6S-31, FOB, 880 Front Street	619 231-1122
San Francisco, California 94102	450 Golden Gate Avenue	415 553-7400
San Juan, Puerto Rico 00918	Rm. 526, USCH & Fed. Bldg., Hato Rey, P.R.	809 754-6000
Savannah, Georgia 31405	5401 Paulsen Street	912 354-9911
Seattle, Washington 98174	Rm. 710, FOB, 915 Second Avenue	206 622-0460
Springfield, Illinois 62702	535 West Jefferson Street	217 522-9675
Tampa, Florida 33602	Room 610, Federal Office Building	813 228-7661
Washington, D.C. 20535	FBI Washington Field Office	202 324-3000

Appendix H
TRAINING IN COMPUTER-RELATED CRIME*

* A major portion of this list was contributed by Carlton Fitzpatrick, Federal Law Enforcement Training Center, (912) 276-2314.

Law Enforcement and Prosecutor Training Programs

1. Adaptive Systems, Inc.
   Contact: Louis P. Carsone, VP
   37 Walnut Street
   Hubbard, OH 44425
   (216) 534-5525

   Program: Training in the investigation and prosecution of computer-related crime. The course involves hands-on work with microcomputers and several case-study problems. Currently, the company has a contract with the Ohio Peace Officer's Training Academy.

2. Center for Criminal Justice Case Western Reserve University
   Cleveland, OH 44106
   (216) 368-3308

   Program: Twelve-hour course that deals with the use and advantages of computers in law enforcement.

3. Central Missouri State University
   National Police Institute
   405 Humphreys Building
   Warrensburg, MO 34093-5119
   (816) 429-4090

   Program: Introductory and hands-on course using microcomputers in criminal justice areas.

4. Cerow Investigations and Consultants
   Attn: Wayne Cerow
   P.O. Box 35428
   Phoenix, AZ 85069
   (602) 978-8000

   Program: Custom, on-site training courses available in a wide variety of law enforcement/investigative applications. Cost negotiable, depending on criteria.

5. Communications Fraud Control Association
   Rami Abuhamdeh, Executive Director
   P.O. Box 23891
   Washington, D.C. 20026
   (703) 848-9768

   In cooperation with local law enforcement, the association has sponsored training on investigation and prosecution of telecommunications fraud.

Criminal Justice Center Police Academy
Box 2296
Sam Houston State University
Huntsville, TX 77341

Program: Two-day course offered on credit card fraud and bank security. Four-day course offered on financial investigation techniques.

Division of Continuing Education
University of North Florida
P.O. Box 17074, Pottsburg Station
Jacksonvile, FL 32216

Program: Two-day seminar on assets protection to ensure computer security, prevent white-collar crime, and reduce employee theft.

FBI Academy
Economic and Financial Crimes
Training Unit
Quantico, VA 22135
(804) 640-6131

Investigative Techniques of Computer-Related Crimes" Program: An in-depth, three-week course on the investigation of computer-related crimes offered and taught at the Academy. The curriculum for this course is centered on the investigation of automated financial record systems using a simulated banking environment.

"Introduction to Computer Related Crime" Program: An introductory, three-and-a-half-day course taken to the training recipients and tailored somewhat to their specific needs.

Federal Law Enforcement Training Center (FLETC)
Computer Fraud and Data Processing
Investigations Training Program
Glynco, GA 31524
(912) 276-2314

"Computer Fraud/Data Processing Investigations Training Program" Program: An in-depth two-week course on computer-related crimes taught at the training center. The curriculum focuses on three major areas: principles of computer data processing, legal concerns, and case development. Through a training blend of theory and practical exercises, including simulated case problems, the students will learn the basic tools necessary to investigate computer-related crimes.

10. Institute of Police Traffic Management
University of North Florida
4567 St. Johns Bluff Road, South
Jacksonville, FL 32216
(904) 646-2722

Program: An introductory microcomputer workshop for the police manager. Advanced courses available using the Condor DBM or Supercalc 2.

11. Institute on Organized Crime
16400 Northwest 32nd Avenue
Miami, FL 33054
(305) 625-2438

Program: Computers in investigation and crime.

12. International Association of Chiefs of Police
Thirteen Firstfield Road
P.O. Box 6010
Gaithersburg, MD 20878
(301) 948-0922

Programs: Investigation of computer fraud, police computer applications and management, developing and managing computer-aided dispatch systems, developing police computer capabilities, telecommunications. Courses developed for those with no computer background or one year's experience.

13 Koba Associates, Inc.
Computer Related Crime Project
2000 Florida Avenue, N.W.
Washington, D.C. 20009

Program: Three-day workshop on the detection, prevention, investigation, and prosecution of computer-related crimes.

14. MCI Communications Corporation
Kevin Houlihan, Director of Investigations
Office of Corporate Systems Integrity
1133 19th Street, N.W.
Washington, D.C. 20036
(202) 887-2160

MCI Communications Corporation offers, upon request, one- to three-day courses for law enforcement officials, prosecutors, and others in the area of telecommunications fraud and related matters.

The topics presented vary, based upon the interest of the target group, but typically include basic telephony (including a description of the

operation of the telephone system), investigative techniques (including an analyais of how and why telecommunications fraud is perpetrated, methods of detection, preparation and execution of search warrants, etc.), prosecutive strategies (including an analysis of applicable state and federal charging statutes), other relevant legal matters (such as the legal requirements for obtaining telephone records, wiretaps, etc., under the Electronic Communications Privacy Act and other statutes), the role of the telecommunications carrier in telecommunications fraud cases, the relationship between telecommunications fraud and other criminal violations, and so on.

The courses and accompanying instructional materials are provided by MCI without cost to criminal justice agencies.

15. National College of District Attorneys
Contact: Karen Townsend, Director of Training
(713) 747-6232

Once a year the College offers a week-long course in forensic evidence. A one-and-a-half hour component of this course is on prosecuting computer crimes. Often the course is part of a roadshow training effort. Other roadshows are possible.

16. The New England Institute of Law Enforcement Management
Babson College, Drawer E
Babson Park, MA 02157
(617) 235-1200

Program: A three-week program that deals with computers as a tool for management.

17. The Pennsylvania State University
Administration of Justice Program
S-159 Henderson Human Development Building
University Park, PA 16802
(814) 863-0078

Program: Introduction to microcomputers and a course focusing on data-base management for more advanced professionals.

18. U.S. Sprint Communications,
Western Regional Division
R. E. "Sandy" Sandquist
1099 18th Street
Denver, CO 80202
(303) 297-5318

At no cost to local law enforcement personnel within the boundaries of U.S. Sprint's western regional division, Mr. Sandquist will provide training in telephone technology and legal issues.

Computer Training Program Available in the Private Sector

1. Adaptive Systems, Inc.
   37 Walnut Street
   Hubbard, OH 44425
   (216) 534-5525

   Programs: Introduction to microcomputers, hands-on training in basic and advanced PC/MS-DOS operating system commands, telecomputing, and client-specific contract training.

2. The American Institute for Professional Education
   Carneqie Bldg., 100 Kings Road
   Madison, NJ 07940
   (201) 822-1240

   Programs: Three-day session on the operational and technical aspects of data communications (more experience as electronic data processor needed). Also offered is a seminar on the legal aspects of software acquisitions.

3. American Management Associations
   135 West 50th Street
   New York, NY 10020
   (518) 891-0065

   Programs: Fundamentals of data processing for the non-data processing executive, concepts of application prototyping to save time, minicomputers, or software.

4. Arthur Anderson and Co.
   69 West Washington Street
   Chicago, IL 60602
   (800) 323-0815

   Programs: Variety of courses ranging from accounting and finance, auditing, and information systems to specialized industry courses.

5. Battelle Seminars and Studies Program
   4000 N.E. 41st Streeet
   P.O. Box C-5395
   Seattle, WA 98105
   (800) 426-6762

   Program: Seminar on managing computer projects.

6. Center for Advanced Professional Education
   1820 E. Garry Street., Suite 110
   Santa Ana, CA 92705
   (714) 261-0240

   Programs: IBM PC implementation in organizations, UNIX, networking IBM PC, database systems, communications, SNA, and PBX/CBX.

7. Cerow Investigations & Consultants, Inc.
   P.O. Box 35428
   Phoenix, AZ 85069
   (602) 978-8000

   Programs: Establishing and training corporate computer-related investigation teams. Developing computer security awareness programs for corporations.

8. Computer Security Institute
   43 Boston Post Road
   Northborough, MA 01532
   (617) 845-5050

   Program: A selection of two-day computer security workshops and optional one-day seminars.

9. Continuing Engineering Education
   George Washington University
   Washington, D.C. 20052
   (202) 676-6106

   Programs: Local area networks, data communications, telecommunications, spread spectrum systems. Experience or a degree in engineering or science needed.

10. Data-Tech Institute
    Lakeview Plaza
    P.O. Box 2429
    Clifton, NJ 07015

    Program: Three-day seminar on local area networks (LANs). Need some previous experience in this area.

11. EDP Auditors Foundation
    373 South Schmale Road
    Carol Stream, IL 60188

    Programs: Audit, control, and security of computers, mainframes, and micros. Sessions taught in both English and Spanish.

12. The Hartford Graduate Center
    275 Windsor Street
    Hatford, CT 06120
    (203) 549-3601

    Programs: Computer use, languages, system development, data base.

13. Institute for Advanced Technology
    6003 Executive Boulevard
    Rockville, MD 20852
    (800) 638-6590

    Programs: Wide variety of seminars on such topics as improving performances and productivity, data communications, DBM series, EDP operations, software engineering, PC, and an IBM series.

14. Institute for Communications and Information Management
    P.O. Box 8
    Pine Mountain, GA 31822-0008
    (800) 247-1212, Ext. 432

    Programs: AT&T offers courses in communications management, integrating LSNs, data processing, data communications, UNIX, and office automation.

15. Institute for Professional Education
    1515 North Courthouse Road, Suite 303
    Arlington, VA 22201
    (703) 527-8700

    Programs: Three-day seminars on personal computers, computer graphics, audit and security, database design, data communications, systems analysis, and micros.

16. MIS Training Institute, Inc.
    498 Concord Street
    Framingham, MA 01701
    (508) 879-7999

    Programs: Tutorials on IBM's operating systems, UNIX, LANs, languages, data security, security and control, and a variety of other concurrent technical sessions.

17. MTI Teleprograms Inc.
3710 Commercial Avenue
Northbrook, IL 60062

Offers training films, slide programs, and pamphlets for rent or purchase. Subject material deals with protection of proprietary information.

18. National Training and Computer Project
c/o Illinois Renewal Institute, Inc.
500 South Dwyer Avenue
Arlington, Heights, IL 60005
(312) 870-4170

Program: Training and computers: How to teach people to use computers.

19. Personal Computer Management Association
11928 North Earlham
Orange, CA 92669-3547
(714) 532-6717

Programs: Hands-on seminars on IBM PC DOS techniques, implementing and controlling PC networks and LANs, micro-to-mainframe integration, networking personal computers, and supporting and controlling PC users.

20. Software Institute of America, Inc.
8 Windsor Street
Andover, MA 01810
(617) 470-3880

Programs: Seminars on data communications and networking for personal computers and micros, operating systems, and software.

21. U.S. Professional Development Institute
Managing Microcomputers in Government
1620 Elton Road
Silver Spring, MD 20903
(301) 445-4400
FTS (202) 445-4400

Programs: Using micros for government management, financial managment, microcomputer integration in government, small computers in government, UNIX and C programming, telecommunications, and software development.

22. U.S. Small Business Administration
1441 L Street, N.W.
Washington, D.C. 20416

Program: Seminars on computer security at their offices throughout the country. These courses are designed for the small business interested in computer security guidelines for their systems.

23. William A. Crowell
DAS/FS Department of the Treasury
Room 2434
15th Street and Pennsylvania Avenue, N.W.
Washington, D.C. 20220

Program: Protecting Electronic funds and securities transfers.

Appendix I
LIST OF PARTICIPANTS

Mr. Anthony Adamski, Jr.
Federal Bureau of Investigation
Financial Crimes Division
Room 3841
10th Street and Pennsylvania Avenue, N.W.
Washington, D.C. 20535
(202) 324-5594

Judge H. Jeffrey Bayless
City/County Building
1437 Bannock Street
Room 205
Denver, CO
(303) 575-2797

Mr. James R. Caruso
AT&T Corporate Security
Room 4B03
20 Independence Boulevard
Warren, NJ 07060
(201) 580-8304

Mr. Wayne Cerow
Cerow Investigations and
Consultants, Inc.
P.O. Box 35428
Phoenix, AZ 85069
(602) 978-8000

Mr. William F. Chapman, Jr.
Criminalist
Jefferson County Sheriff's Department
17900 West 10th Avenue
Golden, CO 80401-2697
(303) 277-0211

Dr. James Conser
Assistant Dean
College of Applied Sciences
Youngstown State University
410 Wick Avenue
Youngstown, OH 44555
(216) 742-3321

Mr. James Fitzpatrick
Assistant District Attorney
Philadelphia District Attorney's Office
Economic Crimes Section
1421 Arch Street
Philadelphia, PA 19102
(215) 686-8735

Mr. Robert J. Humphreys
McCardell, Downelly, Bensen
& Ahern, P.C.
2840 South Lynnhaven Road
Virginia Beach, VA
(804) 486-7055

Detective Calvin Lane
Computer Crime Unit
Baltimore County Police Department
400 Kenilworth Avenue
Towson, MD 21204
(301) 887-2225

Mr. Mickey Litt
Economic Crimes Section
Philadelphia District Attorney's Office
1421 Arch Street
Philadelphia, PA 19102
(215) 686-8734

Mr. J. Thomas McEwen
Institute for Law and Justice, Inc.
1018 Duke Street
Alexandria, VA 22314
(703) 684-5300

Mr. Ken McLeod
504 Edison Avenue
Buckeye, AZ 85326
(602) 935-7220

Detective Michael J. Mullen
Economic Crime Unit
Philadelphia Police Department
319 Race Street
Philadelphia, PA 19106-1894
(215) 592-5592

Sergeant William F. Nibouar
Technical Crimes Investigation
Maricopa County Sheriff's Office
102 West Madison
Phoenix, AZ 85003
(602) 256-1000

Mr. Donn B. Parker
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025
(415) 859-2378

Mr. Daniel J. Piskur
Security Administrator
CompuServe, Inc.
5000 Arlington Centre Boulevard
P.O. Box 20212
Columbus, OH 43220
(614) 457-8600

Special Agent Stephen R. Purdy
United States Secret Service
Fraud Division
1800 G Street, N.W.
Washington, D.C. 20223
(202) 535-5850

Mr. Edward Rapacki
Assistant District Attorney
Middlesex County District
Attorney's Office
40 Thorndike Street
Cambridge, MA 02141
(617) 494-4077

Detective Larry L. Scheideman
Intelligence Division
Lakewood Police Department
445 South Allison Parkway
Lakewood, CO 80226-3105
(303) 987-7370
Electronic Bulletin Board:
(303) 987-7388 at 1200 baud, no parity, and 1 stop bit with 24-hour public access

Detective Philip J. Silverman
Economic Crime Unit
Philadelphia Police Department
319 Race Street
Philadelphia, PA 19106-1894
(215) 592-5592

Mr. Frank Simmons
Manager of Investigations
Cable and Wireless Communications
1919 Gallows Road
Vienna, VA 22180
(703) 734-7140

Mr. Robert Smith
Assistant Attorney General
Office of the Attorney General
10th Floor, State Office Tower
30 East Broad Street
Columbus, OH 43215
(614) 466-6410

Detective Robert M. Snyder
Organized Crime Bureau
Public Safety Department
Division of Police
120 West Gay Street
Columbus, OH 43215-0009
(614) 222-4909

Professor John T. Soma
University of Denver
College of Law
1900 Olive Street
Denver, CO 80220
(303) 871-6295

Ms. Gail Thackeray
Assistant Attorney General
Office of the Attorney General
1275 West Washington
Phoenix, AZ 85007
(602) 542-3881

Mr. Jonathan Budd, Project Monitor
National Institute of Justice
633 Indiana Avenue, N.W., Room 801
Washington, D.C. 20531
(202) 272-6040

U.S. Department of Justice
Office of Justice Programs
National Institute of Justice

Washington, D.C. 20531

Official Business
Penalty for Private Use $300

BULK RATE
POSTAGE & FEES PAID
DOJ/NIJ
Permit No. G-91