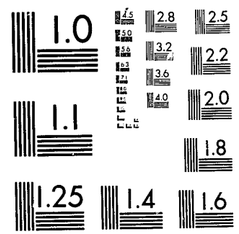

U.S. Department of Justice
Law Enforcement Assistance Administration

WCC
WHITE COLLAR CRIME

APRIL 1980

THE INVESTIGATION OF COMPUTER CRIME

An Operational Guide to White Collar Crime Enforcement

OPERATIONAL GUID[illegible] WHITE-COLLAR CRIME ENFORCEMENT

THE NATIONAL CENTER ON WHITE-COLLAR CRIME

Herbert Edelhertz, Project Director

Clifford Karchmer, Director of Training
and Operations

THE INVESTIGATION OF COMPUTER CRIME

By

Jay J. Becker
Director
National Center for Computer Crime Data
Head, Antitrust Section
Los Angeles County District Attorney's Office
California

Project Monitors:

James O. Golden, Director
Criminal Conspiracies Division
Office of Criminal Justice Programs

Jay Marshall
Criminal Conspiracies Division
Office of Criminal Justice Programs

This project was supported by Grant Number 77-TA-99-0008 awarded to the Battelle Memorial Institute Law and Justice Study Center by the Law Enforcement Assistance Administration, U.S. Department of Justice, under the Omnibus Crime Control and Safe Streets Act of 1968, as amended. 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.

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, D.C. 20402

Stock Number 027-000-00897-6

THE INVESTIGATION OF COMPUTER CRIME

by

Jay J. Becker

TABLE OF CONTENTS

ABOUT THE AUTHOR

Jay J. Becker is head of the Antitrust Section, Los Angeles County District Attorney's Office, and Director of the National Center for Computer Crime Data. The center, which he originally established for the California District Attorney's Association in 1978, is a clearinghouse for computer crime information and studies. He has lectured on computer crime for the Federal Bureau of Investigation, the Utah Attorney General's Office, the National Center on White-Collar Crime at the Battelle Law and Justice Study Center, and numerous computer, security, business, and law enforcement groups in the United States, England, and Bermuda.

His publications on computer crime include editorials in the Los Angeles Times, San Diego Union, San Francisco Examiner, and Honolulu Advertiser; and book reviews in the Washington Post, Security Management, and the Prosecutors Brief. He has also written "Programmed for Crime," a study of the trial of computer crime cases in 2 Los Angeles Lawyer, 8 (1979), pp. 18-31, and is special editor of the upcoming (January 1980) special issue of the Computer Law Journal on Computer Crime.

He received a Juris Doctor degree from Harvard Law School in 1968.

FOREWORD AND ACKNOWLEDGMENTS

This Operational Guide is one of a series developed by the National Center on White-Collar Crime as part of the Center's program of support services to agencies engaged in the prevention, detection, investigation, and prosecution of white-collar crime and related abuses. These Operational Guides are intended for use in actual law enforcement operations, as well as training, on the theory that the best training materials are those which most respond to the day-to-day needs of users who regularly practice their skills. This series evolved parallel with, and as a part of, the Center's preparation of a curriculum for training in the field of white-collar crime enforcement. Its authors are encouraged to express their own views and, as might be expected, different and even conflicting perceptions and approaches will be found among the National Center's Operational Guides and other publications.

Special mention should be made of the support and encouragement of James O. Golden, Director, and Stephen Cooley, Deputy Director, of the Criminal Conspiracies Division of the Office of Criminal Justice Programs, Law Enforcement Assistance Administration, and of Mr. Jay Marshall who is our LEAA Project Monitor. Last, we gratefully acknowledge the invaluable support of members of the Battelle Law and Justice Study Center staff, and particularly that of Charleen Duitsman, Cheryl Osborn and Ingrid McCormack who typed our manuscripts, kept our files, and did all those things without which this series could not have been created.

Herbert Edelhertz
Project Director
National Center of White-Collar Crime

THE INVESTIGATION OF COMPUTER CRIME

by

Jay J. Becker

I. INTRODUCTION

It is important that we first recognize and agree that computer crime is worth studying. Not everyone agrees. Oddly enough, it is often those people who have the most knowledge of computers, people who work with them, who ridicule the idea.

Commenting on S.B. 240, the Ribicoff Federal Computer Systems Protection Act, Jon Taber, an IBM employee (speaking in a non-representative capacity) said:

> Senate Bill S240 is an ill-formed and dangerous law that must be rejected. The bill is fundamentally flawed. The fundamental problem is that it defines an abstraction, "computer crime," as a crime rather than specific acts. Compare "computer crime" with "filing cabinet crime" to make this flaw apparent. Computer crime (or filing cabinet crime) beclouds specific criminal acts, and non-criminal acts, with a trope drawn from the instrument of the acts.

Others have asked why we study computer crime and not gun crime, auto crime or television crime. Throughout this manual this question is addressed. In doing so, we also recognize that we must keep in mind that the computer is the tool or instrumentality of crime, and that we are dealing with old crimes in new forms--forms which present special challenges to those involved in the prevention, detection, investigation, and prosecution of white-collar crime. Thus, while we talk of "computer crime," we should think of it as "computer-assisted crime."

From before the investigation begins to long after it ends, the fact that there's a computer involved means new and different headaches for the investigator. Thus, we have listed some of the more obvious problems that accompany the computer and

suggested possible solutions. Like aspirin, they've proven useful to some people, but hardly qualify as panaceas.

We can generalize from the specific investigative problems computers present and from the characteristics of computers today and list several distinctions which pervade all aspects of the investigation of computer crime.

A. Omnipresent Applications

The number of computers in use, the widespread nature of their use, and the importance of this use to the functioning of our economy and our government, mean that crimes involving computers have far greater potential importance than crimes involving any other type of technology.

Doomsday scenarios are easy to imagine.

Louis Charbonneau, in Intruder[1] (a novel), vividly portrays the consequences of one crazed man gaining access to a small city's computers. He controls the electricity, flow of traffic, dissemination of credit information, and for a while, all access to the computer itself.

Donn Parker, computer crime's most indefatigable chronicler, has voiced concern about the possibility of financial computer terrorists who could wreak havoc with the international monetary system if they gained control over the computer-based systems used to transfer money around the world.

Our government security is based on sophisticated computer defense systems. Though considerable effort has gone into safeguarding these systems, questions about their vulnerability are real. In Computer Capers, Thomas Whiteside reports that it took two researchers but 2 1/2 hours to penetrate the security of a system which had been proposed by the Air Force Data Services Center as a means of handling secret computerized defense information.[2]

---

[1]See attached for footnotes.

B. Intellectual Implications

In addition to the changes in business and government practices resulting from computer use are changes in some four basic assumptions about our world. Traditionally, the concept of "intangible" property was a minor exception to the rule that only "tangible" things could be property. It was sufficient to create areas of law like copyright, trade secrets, and patents, and to handle these exceptions. Suddenly, the law must deal with all sorts of new questions because programs, data, and other information associated with computers appear to be "intangibles" and don't fit neatly into the standard exceptions. Yet they have too much commercial value to simply be ignored. Where laws are based on pre-computer assumptions (like definitions of crime and rules of evidence), these intellectual problems can be severe.

New words, new organizations of people, production and paperwork, and new methods of analysis (all of which have accompanied the growing use of computers) are still another aspect of the intellectual challenges the computer brings in its wake.

This manual tries to avoid conventional computer expertise and jargon. Too often the investigator will encounter a number of foreign terms as soon as he or she begins to discuss computer crime with an expert. Glossaries abound, and several of the texts listed in this operational guide offer more than adequate ones. In the long run, however, none of these is as valuable as simple patience and bravery.

The patience is necessary if the investigator is to ask enough questions to get the expert to translate from "computerese" to English. (Of course, the investigator will have to resist the temptation to talk "law-enforcement-ese" to the expert, making communication even more unproductive.)

The bravery required of the investigator consists of being able to simply say "I don't understand. Explain it to me."

C. Sociological Complications

Most of the world lacks sufficient information to react with strict rationality to the growing importance of computers and their growing effects on our thoughts. Consequently, we have developed some irrational reactions to computers which further complicate the field of computer crime. Myths have developed about computers which affect how judges sentence, how newspapers report, how businesses react, and how criminals misbehave.

When a computer operator inserts a car key in a computer memory and short circuits it because of an "overpowering urge" to shut the computer down, it seems clear that more than the profit motive is involved. Though there are several myths with which we surround the computer, they all boil down to the idea that the computer isn't something we can really bring our minds to understand.

In this manual, the sociological complications of computer crime are dealt with in two ways. First, we point out these complications, referring to them with the generic term "computer mystique." Second, we assume that the reader shares the common and normal susceptibility to some aspects of the mystique. As a consequence of this assumption, we have tried to be as specific as possible about the factual and intellectual problems presented by the computer. The more the investigator focuses on these, the more he or she will be able to feel comfortable with the computer and thus develop something resembling an immunity to the mystique.

It is important that the investigator recognize the danger of the mystique. If we shy away from a problem because we fear we won't be able to solve it, we are defeated before we start.

The problems investigators are likely to face are more often novel than complex, more often complex than unsolvable. The scoffers who doubt the existence of this myth, or the pessimists who doubt that the problem can ever be resolved, are

invited to read "Computer Crime Fighters Go To Boot Camp" (Appendix 1), which describes how 23 prosecutors learned to stop worrying and love the computer.

They just dug in and focused on the problems at hand, which is what we will now do.

II. INITIATION: GETTING REPORTS OF COMPUTER CRIME

A. Unique Aspects of Computer Crime

1. Low Reporting Rates. When Stanley Rifkin was arrested for the theft of $10.2 million from the Security Pacific Bank in Los Angeles, bank personnel minimized the involvement of computers. One vice president called the theft "no more than a sophisticated burglary." Another said "the alleged fraud . . . did not involve the use of a computer." A third said "no hardware more sophisticated than a telephone was involved in the Rifkin theft."

At the base of all these comments was the belief that, according to Senior Vice President Dick Warner, "the banking industry operates on the basis of computer activities. We are concerned that people do not unnecessarily impugn the integrity of those computers."

In England, a programmer stole a considerable amount for several years before being caught. After he was confronted by the victim's board of directors, he threatened to expose the weaknesses of the company's computer system and ruin the company's reputation for efficient management of its affairs unless the company wrote him a letter of recommendation (so that he could get another job in the programming field). The company knuckled under, wrote him the letter, and the programmer went on to commit a similar theft against his new employer.

These examples merely highlight the widely quoted statistics that only 15 percent of all computer crime is reported to

law enforcement authorities. They suggest that in addition to all the problems we face in attempting to get the business community to report white-collar crimes in general, there is an added reluctance to report crimes involving computers. In addition to the fear of losing face, the businessman or woman contemplating reporting computer crime may simply conclude that the likely benefits to accrue to his or her company are not sufficient to justify the costs.

The costs referred to involve the time it takes to brief investigators and cooperate with the investigation, the disruption of ordinary procedures to supply the information necessary to investigate the crime, and the court time necessary for testimony should the case go to trial. To the extent that a computer case is more complicated than other white-collar crime cases, the business person has more reason to fear that these costs will be even greater if computer crime is involved.

There is also considerable skepticism in the business community as to the effectiveness of the criminal justice system, and a fear that even with full cooperation the criminal will not be arrested, convicted, or adequately sentenced to justify the victim's involvement in a criminal investigation and trial. Again, in the area of computer crime, there would appear to be more reason for a businessman or woman to adopt this point of view than in other areas. Experts at the Federal Bureau of Investigation say only one of 22,000 computer criminals goes to jail. They estimate that only 1 percent of all computer crime is detected, only 14 percent of that is reported, and only 3 percent of those cases ever result in jail sentences. The victim of a computer crime may also assume that the local law enforcement agency has no investigators capable of investigating a computer crime, that there are no prosecutors capable of adequately taking such a case to trial, and that there are no judges sufficiently sophisticated to conduct the trial and sentencing in such a case.

Even where management responsible for making such decisions is in favor of reporting computer crime, those employees who are most likely to detect computer crime may hinder reporting. The computer industry has not developed ethical standards reaching even the arguably minimal level of consensus that exists in the area of white-collar crime. Though it is clear that taking a typewriter is theft and taking a pencil is not, no similar dividing line appears to exist between using $2 worth of computer time and $200,000 worth. Considerable disagreement exists throughout the industry on just about every ethical question which has been raised.[3]

2. Different Sources of Information. For law enforcement officials, part of the problem in determining the existence of computer-assisted criminal offenses is the fact that different professional people are likely to be the source of reports of potential computer crime cases. Systems analysts, auditors, and programmers--people seldom seen in a police station--have an important role in communicating both the possibility of a computer crime and the dimensions of that crime.

The lack of prior personal contact between these people and law enforcement authorities constitutes a further barrier to reporting. The "old boy" network which links law enforcement personnel to the business world in other criminal containment areas has not yet taken form.

B. Approaches to These Problems

1. High Profile. If your office has an interest in investigation of computer crime cases because of its belief that the business community and the consumers (who bear the business community's losses) deserve this protection, let your community know it. In the process, don't forget to let other local law enforcement agencies, as well as the members of your own office, also become aware of your unit's capability and

interest in investigating these sorts of crime. Speeches to professional, civic, legal, and other groups, press releases, and whatever other public-relations approaches your office uses, can be mobilized to report the completion of a course in the investigation of computer crime, your office's concern with the problem, and steps business can take for self-protection.

2. Becoming Familiar with the Different Sources of Information. As a narcotics officer cultivates snitches, a computer crime investigator must develop contacts among those people likely to report computer crimes. In addition to speeches before various professional organizations whose members are involved in the use of computers, membership in some of these organizations may be useful. Among the organizations with an interest in computer crime are the following:

- ACM Association for Computing Machinery
  1133 Avenue of the Americas
  New York, NY 10036 (212) 265-6300

- AICPA American Institute of Certified Public Accountants
  1211 Avenue of the Americas
  New York, NY 10036 (212) 575-6200

- ASIS American Society for Industrial Security
  2000 "K" Street N.W.
  Washington, D.C. 20006 (202) 331-7887

- DPMA Data Processing Managers Association
  505 Busse Highway
  Park Ridge, IL 60068 (312) 825-8124

- EDPAA EDP Auditors Association
  c/o Gerald Meyers
  7024 Edgebrook Ln.
  Hanover Park, IL 60103 (312) 822-4994

- EDPAF EDP Auditors Foundation
  c/o Dr. Martin Bariff
  P.O. Box 8184
  Fountain Valley, CA 92708 (204) 243-8601

- IIA Institute of Internal Auditors
  249 Maitland Avenue
  Altamonte Springs, FL 32701 (305) 830-7600

- NCCCD National Center for Computer Crime Data
  320 West Temple Street, Rm. 540
  Los Angeles, CA 90012 (213) 974-3955

The National Center for Computer Crime Data maintains liaison with many of these groups and files of experts and consultants who may be of value. See Appendix 2 for more details.

3. Trying to Change the Public Mood. Without pretending to be able to remake the world overnight, the investigator should take those opportunities that he or she has to address the problems of computer crime to educate the public and the business community about both the legal and the moral obligations of the business community to report computer crime. In this context the investigator should be aware of both federal and state laws which require, or might foster, greater reporting of computer crime.

The Foreign Corrupt Practices Act (15 U.S.C. 78 dd 1-78 dd) only applies to foreign corrupt practices. It requires that every reporting company "make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer." Where computer crimes cause loss to a company, and this loss is hidden, the F.C.P.A. may apply.

Misprision of felony (18 U.S.C. 4) (the failure to report a felony to the authorities); compounding a crime (18 U.S.C. 1001) (the knowing concealment of a crime); and the various reporting requirements of specific regulations like those of the Securities and Exchange Commission or the Federal Deposit Insurance Corporation all create a series of legal sanctions against failure to report.

In most states compounding a felony is a crime, and state regulatory agencies may require reporting similar to that required by federal authorities.[4]

There is also a practical/moral argument to be made for reporting. In view of the current post-Watergate stress on honesty in business and government, the company that fails to disclose computer crime, and is later found out, may be in far worse shape than if it had simply faced up to its reporting responsibilities in the beginning.

III. PRELIMINARY PLANNING: GETTING READY TO APPROACH THE COMPUTER

A. Unique Aspects

1. New "Pigeonholes." To begin the analysis of a potential computer crime, one must have a general familiarity with the common types of computer crime and the laws that may apply to these types of crime. Frequently an understanding of the business practices of the victim company will be necessary as well. It will also be necessary to look at different types of evidence, and to speak with people occupying different positions in the victim's organization to gain the evidence necessary to completely investigate a computer crime.

2. The Necessity for Expert Assistance. One can no more investigate a complex computer crime case alone than one could investigate an art forgery, a securities swindle, or an accusation of death resulting from medical malpractice. The combination of technical, business, and legal complexities means that other experts may be needed to explain the computer context, the business context, or even the legal context. It is important that the investigator know where to find these experts, what types of questions they can be expected to help him or her answer, and how to understand their responses.

B. Approaches to These Problems

1. Develop a Framework for Understanding Computer Crime. In order to best understand experts who describe the mechanisms and the effects of computer crimes, and also to develop your own sense of whether a computer crime has taken place, it is important to have a clear understanding of the context of computer crime. This understanding should include a working knowledge of each of the following:

a. What are the vulnerable points of a computer system? Each of a computer system's component parts can be seen as an area of vulnerability:

Input. That part of the computer that takes data about the world outside the computer and "feeds it" to the computer. Input devices, or means of communicating this data to the computer, include punched cards, tapes, discs, cassettes, etc. The type of information that may be contained on input data include records of payments made, records of debts to accounts, invoices that are to be paid, traffic tickets, etc.

Programming. This is the part of the computer that manipulates data which is "fed" into it through the input devices. Programming is responsible for reducing your checking account balance by the amount the input indicates you have used, increasing your savings account balance by the amount the input data indicates you have deposited, calculating your withholding tax and subtracting it from your paycheck, etc.

Software. When people use the word "software" they generally mean programming. Strictly speaking, software includes "documentation" (which we define in Section c

below) and excludes those programming capabilities which are manufactured into the "hardware."

Operating System. This part of the computer deals with control of the operation of the computer. Security of the data in the computer, coordination of the different tasks the computer programs may be processing at the same time, and coordination between one computer and another computer are handled by the operating system.

Data Base. Most business computers have a data base. This may consist of names, addresses, and account statuses for hundreds of thousands of members of a book club, data about transactions with all of a company's suppliers or buyers, an employee payroll file, etc.

Output. This is what the computer produces after it has performed the operations dictated by the programming on the input or the data base. Paychecks, management reports, and bills are all types of output. The output may be in the form of paper, microfilm, TV screen images, tapes, cassettes, etc.

Hardware. This is the generic name for the computer itself and refers to all of the physical components of the system, but not the software.

Communications. More and more computers are connected to other computers and to remote terminals. The means by which they are connected, usually telephone, microwave, or similar devices, are called communications.

b. What are typical threats at each point of vulnerability?

Input.

Addition of fraudulent data: such as non-existent employees or invoices for goods that were never delivered.

Alteration of data: like changing the value of a stock from $1.50 a share to $200.00 a share, or changing a student's "C" grade in Computing Science to an "A-."

Omitting input data: such as removing a traffic ticket from the records to be input to the computer, or a check which would be debited to one's account.

Programming. Changing the programming so that all fractions of cents are credited to an employee's account, the computer continues paying an employee after termination of his or her employment, or the credit limit is removed from a person's credit card account.

Software. In addition to the examples offered for programming, there is the threat of misappropriating the software for unauthorized use, or selling it to another computer user.

Operating System. Getting time on the computer without proper authorization, reading confidential information which is normally kept inaccessible by the operating system.

Output. Pressing a REPEAT button on a check printer and producing a number of duplicate checks in the same name, destroying a report indicating an overdrawn account, stealing a printout of a competitor's major customers.

Data Base. Destroying a data base for revenge or as a protest, getting information from a data base to obtain an advantage in competition with the data base's owner, stealing the data base and holding it for ransom.

Hardware. Bombing, shooting, burning, flooding, or stealing the computer or part thereof.

c. What types of records will you be looking for?

(1) Documentation. Ideally the documentation maintained in a computer center will thoroughly describe every aspect of the computer system, from the initial purpose for which it was developed to a list of every type of output that it produces. The word "ideally" is used advisedly because documentation practices vary from phenomenally obsessive and complete to non-existent. The major types of documentation are as follows:

- Systems documentation--information which describes the design and operation of an organization's entire computer system.
- Program documentation--more specific information which is used to interpret and make changes in the programming of the system.
- Operations documentation--information concerning the operation of the computer, including information about the various functions of the operating system.
- User documentation--information provided to the department within a company or government agency that actually uses the computer system.
- Vendor documentation--information provided by a manufacturer so that the purchaser of a computer

system or service can operate the system or service.

(2) Other Paperwork. As in any white-collar crime investigation, other documents may prove useful. For example, a document retention form can serve as a quick index to those documents maintained by the company which may be of assistance to you. Particularly valuable will be graphic representations of the computer configuration of the business or agency you are involved with. The configuration is the sum total of the computers, input devices, output devices, and telecommunications devices, all of which constitute a company's system. The parts of the system may be located in widely separated geographic areas, even internationally (and, unfortunately, in some situations the crime may have been committed from any point in the computer system). An organization chart indicating the job titles and responsibilities of those people in the data processing department is another key to determining who may have committed the crime, and who is most likely to be able to answer your questions as to specific aspects of the company's system.

d. Who can you talk to?

The internal auditor is an employee of a business who has as his main function the establishment of management controls for the business systems. Often this responsibility extends to the company's computer system. "Controls" is the word used in the auditing profession to denote rules and practices whereby the components of the business run smoothly. Thus, it is the internal auditor's task to see that the computer system is not being used to commit crimes and that it

is reasonably secure from attempts to use it to commit crimes. To do this, an auditor has a variety of testing procedures to apply to the systems. Appendix 4 demonstrates the extensive attention that an internal auditor should pay to the computer system. As a result of this attention, the auditor may well be able to detect irregularities in the system before the businessman has discovered any loss.

The external auditor works for an accounting firm and is customarily called in by a company to provide impartial analysis of its systems. Where the internal audit capacity is undeveloped in a company, or where there is a question as to the honesty of an internal auditor, an investigator may want to call upon an external auditor to help analyze a suspect computer system operation.

The systems analyst also has a concern for the efficiency of the computer system. His concern is less with the detailed checks than an internal auditor uses, and more with the ability of the computer system to accomplish its computing tasks in an accurate and economical way. The systems analyst usually has substantially more understanding of the machinery of the computer system. His help will probably be necessary to fully explain the computer mechanisms through which the irregularities detected by the auditor have been accomplished.

The security officer--different companies have enormously varying job descriptions for members of the security department. There are banks whose security department does nothing more sophisticated than make sure that nobody draws a gun. There are security

officers who have made intensive and sophisticated studies of computer crime, and take responsibility for development of secure systems and ongoing investigation as to their continued security. Where questions of physical security are involved, such as the possibility of break-ins to the computer center or unauthorized individuals having access to the computer, security personnel are likely to be of assistance.

2. Be Aware of Applicable Law. To investigate a computer crime, like any other crime, it is necessary to know the elements of the crime one seeks to prove. Although most computer crimes will fit under the general definition of theft or malicious mischief at the state level, difficult legal questions may arise. The investigator should be aware of any state laws specifically related to computer crime, and whether any federal laws apply.

By October 1979, ten states had passed computer crime legislation modeled more or less closely after the Federal Computer Systems Protection Act.[5] Thus, more and more the investigator must anticipate the possibility of basing the investigation of a computer crime on the definitions contained within the computer crime laws as an alternative to proceeding under general criminal statutes. Without exhaustively discussing these computer crime laws, several points should be considered in analyzing any such laws:

- Punishments--Does the bill allow for misdemeanor treatment of less significant computer crime cases? What are the maximum penalities?
- Does the bill explicitly allow prosecution of a computer thief under any of the pre-existing statutes which might have applied to his or her criminal activity?
- How is "computer" defined? Are such things as "pocket calculators" included?

- What treatment is accorded intangibles that may be the subject of theft. Some statutes simply define information as property. In contrast, others use the term "data" to cover some of the same territory.

Illustrative of the problems that have arisen in states lacking computer crime bills are the following:[6]

In Wisconsin students who stole time from the university computer could not be prosecuted since no loss to the victim resulted under Wisconsin laws. In another state there was considerable doubt whether that state's malicious mischief statute, prohibiting damage to "real and personal property," covered erasure of the contents of a computer disc. There was no precedent on the question of whether changing polarization on a disc constitutes damage to real or personal property.[7]

In a California case, People vs. Ward, the court suggested in dictum that information not protected by trade secret definition could not be the subject of theft.[8] Also in California, a municipal court judge challenged the prosecutor to establish that he had made out a case of grand theft. The prosecutor had adduced testimony to the effect that a computer tape containing a computer program had been sold for more than $1,000, but the judge asked the deputy to brief the point that the tape itself was worth less than the $200 jurisdictional limit in California.[9]

3. Develop a Written Investigation Plan. More than in any ordinary investigation, a written plan for the conduct of the computer crime investigation is a necessity. The plan should involve the names of the areas, persons, documents, files, and other relevant aspects of the case which are to be investigated. It should include investigation of the company's background, prior crime problems it has experienced, provisions to gather organization charts, functional flow charts, the job

descriptions of its employees, the company's financial statements, and its personnel files.

The plan should be as complete and as organized as possible. The investigator should be aware of the possibility that the document will be used at trial, and thus should attempt to make it clear enough for a juror or judge to understand how the investigation was initiated and conducted.

IV. COLLECTION: GATHERING THE EVIDENCE

A. Unique Aspects

1. The Nature of Computerized Evidence. Several aspects of computerized evidence have direct bearing on the investigator's task. Evidence in a computer is much more "dense" than in any other information system. That is, a single computer tape can contain as much information as a shelf full of books. Consequently, the ease of destroying the information is much greater and the value of the information to a potential thief is greater as well. Furthermore, much of the information is not visible without the use of some device to translate it from electronic impulses to print. Being invisible, the information is also more subject to "booby traps" or illegitimate programming designed to destroy the information should an investigator attempt to reproduce it.

2. The Nature of the System. The computer system itself is dynamic: it consists of information and programs within a computer that is usually in operation. It may not be possible to gather the information one wants out of the computer without shutting down the business operation which the computer has been set up to run. Furthermore, the data on the magnetic tapes, discs, and other storage media cannot be used to produce the hard copy reports that were produced except through use of the same programs and hardware. And while there are many areas

of computer compatibility, one cannot in general obtain any information from a tape or disc unless one has compatible systems and usually a similar computer model. A further practical problem for the investigator is the enormous volume of evidence that a computer center may contain. In the Equity Funding case, some 3,000 reels of computer tapes were potential evidence.

3. Other Problems. The type of evidence which the investigator will want to look at and possibly seize are different than in the normal investigation. Documentation is the most common form of evidence, other than the computer tapes, discs, and other storage media. In unusual cases, the equipment itself might be required. The complexity of the computer case may well make it much more difficult to specify the instrumentality of a computer crime before an investigation has begun. Thus, a certain amount of "fishing" may be necessary to understand how it is that the crime in question was committed. Likewise, the complexity of the crime involved may make it hard to determine who the potential defendants are in certain cases. Thus, the investigator must gather information without tipping off the defendants and enabling them to cover their tracks.

4. Legal Difficulties. Each of the approaches to evidence collection described below has its difficulties:

a. Consent searches. Where the complexity of the case makes it hard to identify the crime perpetrators, a request for a consent search may be counterproductive if it alerts the criminal and affords him or her the opportunity to destroy evidence.

b. Search warrant. Where surprise is desired, a search warrant may seem preferable to a consent search. Few

judges have ever signed a search warrant involving the technical proof of probable cause which may well be presented in a search warrant for a computer system. Additionally, judges have seldom had the opportunity to fashion a search warrant with the sorts of provisions needed to protect evidence once the investigator has gone to the location of a computer system. The requirement that the items to be searched must be narrowly and specifically defined may require an enormous amount of description for the investigator in order to cover each component of the computer system which he seeks to inspect or seize. The affiant in an application for a search warrant will often be a technician, and his or her affidavit may well be written technically.

c. Right to privacy. Whatever the method used to gather evidence from the computer system, the right to privacy in personal information contained in the computer system may present additional problems.

B. How to Meet the Problems

1. The Nature of Computerized Evidence and the Computer System. The major investigative technique is simple awareness. Keeping in mind the problems outlined in Part A of this section, particularly those of a technical nature, will often be sufficient to dictate the appropriate response in a computer crime investigation.

Variables such as whether the complaining witness is someone who can be trusted, whether the employees working in the computer center can be trusted, whether the existence of a law enforcement investigation is already known to many individuals in the company, all will have a significant effect on the course of action one takes when going to actually seize the evidence in question. Nonetheless, some general procedures may be suggested:

- Check with the victim and find out to what extent there are back-up copies of the tapes or other data storage media which you seek to inspect or to seize. It cannot be assumed that the back-up copies are identical to those presently in use, since there is a real possibility that the computer thief will not change the back-up copies as well as the original copies. The back-up copies are useful to allow the computer system to continue in operation while those copies which were actually in use in the system are removed to be duplicated or seized.

- It may often be desirable, if not necessary, to duplicate the contents of each of the information-storing devices in the computer system, be they tapes, discs, cards, etc., so that subsequent changes in the system do not impair the investigation. When such duplication takes place, make sure that the foundation requirements referred to below in Sections 4 and 5 are strictly observed.

Despite the enormous size of the Equity Funding data base--more than 3,000 rolls of computer data--a copying project was undertaken, and a duplicate of every tape on the premises was prepared as one of the first steps in the investigation. All copying was done on the Equity Funding computer equipment. The originals were transported to a vault away from the Equity Funding scene, and the business was allowed to continue with the duplicate tapes.

Where a large volume of tapes or other media are likely to be seized, preparation should be made ahead of time for the removal and storage of these tapes. (See the discussion below concerning preservation of evidence for further suggestions as to what sort of preparations are appropriate.)

The dynamic nature of the computer system necessitates keeping as many employees whose possible involvement in the crime is unclear away from the computer system for as long as possible. This may be easily accomplished in a small system where the seizure can be completed fairly quickly. In a major investigation, one must consider the possibility of furloughs or other enforced leaves for those employees who are not cleared, and if necessary, convincing the victim to bring in temporary help to run the computer operation while the investigation is ongoing. It may often be necessary to pinpoint those areas of greatest sensitivity and deploy law enforcement personnel to secure these areas when it is not possible to segregate all those employees who may have some role in the computer fraud. Special control systems may be appropriate when a large number of suspect personnel are allowed to continue at work in the computer center. These might include the audit trail with the requirement that no input be made into the machine without a hard copy being produced at the same time.

2. Possible Solutions to Legal Difficulties[10]

a. Consent searches. Where the element of surprise is required, a request to perform a consent search may be accompanied by a prepared search warrant. Thus, if consent is granted, the consenting party will not have time to destroy evidence, and if consent is not granted, the search warrant can be immediately served and no loss of time will accrue. There is good reason to request consent even if you have a warrant. Search warrants for computer environments often pose novel and complex issues, and thus may face rough sledding when they are challenged at an evidentiary hearing in court. If a valid consent to search has been received, the evidence seized is admissible even if the warrant is not legally sufficient. The investigator should take care that consent cannot be seen as the product of the warrant, to assure that evidence seized

pursuant to the consent not be deemed inadmissible because of a taint from the warrant. Don't say, "we've got a search warrant, now will you consent to a search?" if you are trying to maintain an independent justification for the search.

In such cases, the consent should be written. The investigator should thus come with a prepared search consent form which is as extensive in its scope as possible. Cases are quite clear that search pursuant to consent can be no more extensive than the consent. It is far preferable to have written proof of the scope of the consent rather than to chance an adverse determination by a trier of fact (i.e., judge or jury) as to whether the consent covered certain specific areas. The search consent form should generally be as specific as possible, perhaps couched in the same terminology as the request for a search warrant, as well as containing several general provisions enabling the investigator to search in those areas that he or she has not been able to adequately and specifically define. The purpose of the specificity is to preclude the subsequent argument that the person giving consent did not understand the language of the consent to extend to those specific areas which the investigator has searched.

b. Search warrants. It is necessary to exercise even greater care than usual in preparing a search warrant in a computer crime case, mainly because this is a technical area often new and unfamiliar to judges. The investigator should have a detailed affidavit which covers all the technical bases, but which is comprehensible to someone who knows nothing about computers. The technical affiant should be available for questioning by the magistrate being asked to sign the search warrant.

Specificity is important wherever possible. Limit the time period to which the records sought to be seized pertain, as well as the number of persons whose records are sought, wherever this can be done without jeopardizing the investigation.

A copy of an actual state search warrant is included in Appendix 5.

Where appropriate, request permission to shut down the operation of the business for a reasonable time to protect the evidence in the search warrant application. Such permission is unusual and will require extensive justification, both factually and legally. Facts must be brought before the court to show that anything short of this drastic step will severely endanger the investigation. Legal authorities, which will have to be provided by the prosecutor assisting in the preparation of the search warrant, will have to show that under these unusual factual circumstances the remedy sought is appropriate.

Additional permission will probably be required before an expert is allowed to touch the victim company's computer. Again, a similarly detailed and persuasive factual and legal argument will be needed before a magistrate grants this unusual permission. Even where the search warrant does provide for the expert's operation of the computer system, it is better to have the consent of the victim and the victim's attorney, where possible, before such operation is begun. There is always a danger that at a later date an objection will be raised along the line that the data was changed by the expert's "meddling" with the victim's system.

c. Right to privacy. Where the information sought relates to individual clients or customers of the victim company, it will be well to get a consent from the victim company to the search based on the company's belief that it is a victim of a crime and that it requires the search of the evidence in question to protect itself from loss resulting from this crime. The specific requirements of this consent will depend on the individual jurisdiction's definition of the right to privacy in such business records and its definition of an exception to this right where the records are maintained by a company which believes itself to be the victim of a crime.

d. Administrative and grand jury subpoenas. Where an industry is regulated, or is otherwise the subject of an administrative or grand jury subpoena, consideration should be given to the use of either of these approaches as well.

e. Emergency seizure. There are circumstances in which an investigator may go beyond the authority of a search warrant or a consent search to make an emergency seizure of evidence. Thus, if the investigator believes that a crime is being committed or evidence destroyed, he or she may go beyond the previously granted authority in order to prevent the crime or the destruction of evidence.

The investigator should exercise great restraint when considering such a seizure. It is possible to hurt the investigation--not to mention the computer operation--by overhasty seizure of evidence. Many computer systems are dynamic, always in operation. Simply stopping the machine might destroy valuable evidence. Where there is a possibility that such seizure will be necessary, someone conversant with the operation of the specific computer system should be part of the investigation team.

V. PRESERVATION: WHAT TO DO WITH THE EVIDENCE ONCE YOU HAVE GOT IT

A. Unique Aspects

1. Technical

a. The possibility that evidence cannot be moved. Although few cases fit into this category, it is possible that the evidence of the commission of a computer crime is not to be found in the programming or the data storage media, but in the machinery itself, perhaps involving communication gear. It may not always be possible to remove the machinery from its

location. Nor may it be possible to keep the machinery from being used.

b. Maintenance requirements of the evidence. It will not be self-evident to the investigator how a computer tape can be preserved. Improper storage may result in warpage or other damage, rendering the tapes unreadable.

c. Volume. Closely related to the general maintenance requirements for computer tapes and other data preservation media are the problems presented by the enormous volume of evidence that may present itself to the investigator at the conclusion of a major seizure.

d. Visual fungibility. Computer tapes are not necessarily distinguishable to the human eye. It is necessary to develop permanent marking systems to keep track of the evidence which is seized.

2. Legal Requirements

A basic requirement for the admission of evidence is proof that "the condition of the object is substantially unchanged."[11]

B. Possible Solutions

1. Technical

a. Immovability of evidence. Where the mountains of evidence cannot be brought to the custodian of evidence, the custodian must be brought to the mountains of evidence. In this rare case, either through consent of the parties involved or by way of court order, one might consider establishing a 24-hour guard in the office of the victim company to safeguard the evidence in question. This procedure was used in the Equity Funding case.

b. Maintenance of evidence. Expert assistance should be sought whenever there is any question as to the storage of materials gained through a seizure of evidence. Such simple matters as how tapes are to be stacked, the ranges of safe temperature in which to maintain them, and possible magnetic, electrical, or other dangers to the security of the data must be considered.

c. Volume and identification. All items which are seized must be carefully indexed. A five-step approach has been suggested to deal with the problems of keeping track of large volumes of computer evidence.[12]

(1) The investigator's initials and the date should be scratched onto each tape reel. The tape canisters which are usually marked to identify the computer tapes they contain are too easily interchanged.

(2) Magnetic discs should be identified with the investigator's initials and date scratched onto the metallic bottom of the disc.

(3) The tape identification number should also be scratched onto the tape reel or disc.

(4) The computer center may have a perforator which can make a "permanent" marking on the tape itself. The tape normally has considerable "leader" or blank tape where such markings can be placed.

(5) Some storage media (e.g., some discs) may not be readily removable. To identify the date in such

a system, it may be necessary to have a printout made of the data stored in the memory component.

2. Possible Solutions to Legal Problems. To establish that the evidence is substantially unchanged, the investigator must be ready to prove a complete chain of custody. Where the seriousness of the case warrants it, a 24-hour guard over the evidence locker, with strict logging procedures whenever the evidence is removed, is ideal. In any case, a system must be developed which carefully maintains evidence of the chain of custody. From the beginning of the search, careful indexing must be maintained of all the evidence which is seized.

The expert assistance that is used to make sure that the evidence is not damaged in storage should be kept available for testimony to that effect, should there be any challenge to the contents of the information at the time of trial.

VI. PRESENTATION: MAKING SURE THE CASE IS NOT THROWN OUT BECAUSE OF SOME FAULT IN THE EVIDENCE

A. What Makes the Area Unique?

1. The Lack of Technical Expertise in the Trier of Fact. Whether judge or jury, the trier of fact is not likely to have any depth of understanding of the components of a computer system.

2. Volume. In many computer cases, the sheer volume of computer media (i.e., documents, tapes, discs, printouts, manuals) offered as evidence can be staggering.

In addition to logistical problems involving document management, there are comprehension problems when a large part of the evidence must be mastered and communicated clearly to the prosecutor so that he or she can, in turn, use it to persuade the judge or jury.

3. Foundation Requirements. For computer media to be admitted as evidence, they must usually qualify as business records which are excepted from the application of the hearsay rule.

The business record exception requires that the following "foundation" requirements be met:

- The computer records were made in the ordinary course of business.
- The information on the records was placed in the computer within a reasonable time after the act or transaction to which it relates.
- The information contained in the computer record comes from a source which is itself reliable.
- The methods and circumstances of the preparation of the computer records must provide reason for the trier of fact to believe that the information is reliable.[13]

Although representing a careful and extensive treatment of the problem of the admission of computerized documents into evidence, the Genser decision is only the decision of the court in one jurisdiction. The foundation requirements will vary from state to state. The sources[14] listed in the endnote offer further information on the admissibility of computer evidence.

B. Possible Solutions to These Problems

1. Repetition of the Investigative Process. The investigator who began his or her case as less than an expert in computers and the detection of computer crime can turn this

initial inexperience to an advantage by maintaining the records of the investigation through each step from initial planning to the completion of the gathering of evidence. Then, in testimony, before the court or jury, he or she should be able to refer to extensive notes and explain exactly what was done in the investigation of the crime. If the investigator cannot explain the investigative steps to a traffic dispatcher, a secretary, or someone else equally untrained, he or she will have difficulty making an effective presentation to the judge and jury.

2. "Librarianship." Effective investigation of a computer crime case will take on certain elements of librarianship. Where the investigator has seized hundreds of reels of tape, he or she must have made detailed notes at the time of the seizure, and must be able to translate those notes for the trier of fact in such a way as to minimize vulnerability to a defense cross-examination attempting to cast doubt as to the accuracy of his or her notes.[15]

3. Foundation Requirements. It is initially the responsibility of the investigator to make sure that witnesses are available to testify to those facts necessary to establish that the requirements listed above under "Foundation Requirements" have been met.

a. Ordinary course of business. As in any business record problem, there must be testimony that the computer printouts were routinely prepared or, if made by a third party such as a service bureau, were ordinarily processed by the third party pursuant to an agreement with the company whose information it is.

b. The appropriate witness. Though some jurisdictions require that only certain individuals with responsibility

for computer centers testify as to records sought to be introduced into evidence, more commonly anyone can testify so long as he or she is found by the court to be familiar with the computerized records in question and the manner in which they were made.

c. Time of preparation of the records. Most jurisdictions do not require that the computer produced the specific printout, tape, or other record contemporaneously with the event to which it refers. So long as the computer system was changed to reflect the event at the time it took place, the requirement of contemporaneousness is satisfied. Thus if an invoice is keypunched, the computer card fed into the computer, and an electromagnetic record of that invoice is made part of the data base, it does not matter whether the printout reflecting that invoice is made one day, one month, or ten years later.

d. Source of the information from which the computer record was produced. The computer cannot be used to "launder" unreliable information. If it has records of readings from broken gas meters, for instance, the source is not sufficiently reliable for the records to be admitted into evidence.

e. The reliability of the method and circumstances of the preparation of the computer records. This is often the most difficult aspect of the foundation requirement. To adequately establish reliability one must be able to show the following:

- The computer operators were competent, they understood the operation of the computers, and had as their regular duty the job of operating it.

- The type of computer used was accepted in the field as standard and efficient equipment.

- The procedure for inputting and outputting of information was acceptable, and included controls, tests, and checks for reliability and accuracy.

- The mechanical operations of the machine were appropriate.

- The records themselves have meaning and identity.

VII. CONCLUSION

The computer is now an essential and established factor in the functioning of our society. It is already unthinkable that our commerce and manufacturing, our government, or even our social and eductional institutions can operate without it. With the computer's benefits, which are very real, come many dangers--to our privacy, to our ability to knowledgeably control the public and private aspects of our lives, and to the integrity of government operations and delivery of government benefits. This operational guide is offered as one tool for the use of those who seek to contribute to the containment of computer-assisted crime which is an ever-expanding threat to the integrity of our institutions and to the welfare of our people.

ENDNOTES

[1]Charbonneau, Intruder, Doubleday (1979).

[2]Whiteside, Computer Capers, Crowell (1978), pp. 116-126.

[3]See Parker, Crime by Computer, Scribners (1976), pp. 122-141.

[4]Lipson, Compounding Crimes: Time for Enforcement?, 27 Hastings L. Rev. 175-211 (1975).

[5]S. 240, 96th Congress, 1st Session (1979).

[6]See Appendix 6 for a more extensive analysis of these issues.

[7]Personal correspondence with personnel in Wisconsin Attorney General's Office.

[8]People v. Ward, 3 Computer Law Service Reporter, 206 (1972).

[9]Personal correspondence with Fred Stewart, Los Angeles County District Attorney's Office.

[10]Appendix 6 supplements this section.

[11]McCormick's Handbook of the Law of Evidence, 2d ed., Cleary, editor, West Publishing Co. (1972), p. 527.

[12]Coughran, Computer Abuse and Criminal Law, Computer Center, University of California, San Diego (1976), pp. 29-61.

[13]See Monarch Federal Savings and Loan v. Genser, 383 A.2d 475 (1977).

[14]Abelle, Evidentiary Problems Relevant to Checks and Computers, 5 J. Computers and Law 323 (1976); Bender, Computer Law: Evidence and Procedure (1978) (Chapters 5, 6); Freed, Computer Print-Outs as Evidence, 16 Proof of Facts 273; Goger, Proof of Public Records Kept or Stored on Electronic Computing Equipment, 71 ALR 3d 232; DeHetre, Data Processing Evidence: Is It Different?, 52 Chic.-Kent L. Rev. 567 (1976); Sprowl, Evaluating the Credibility of Computer-Generated Evidence, 52 Chic.-Kent L. Rev. 547 (1976); Note, A Reconsideration of the Admissibility of Computer-Generated Evidence, 126 U. Pa. L. Rev. 425 (1977); Monarch Federal Savings and Loan v. Genser, 383 A.2d 475 (1977); Tapper, Computer Law, Chapter 6 (1978).

[15]For complex evidence-handling problems, see National District Attorneys Association's Evidence Tracking Manual (available from the National District Attorneys Association, 666 Lake Shore Drive, Chicago, IL 60611).

BIBLIOGRAPHY

General Works

Becker, Robert. The Data Processing Security Game. Pergamon (1978).

A concise summary of considerations in data processing security. Pedagogic in style, complete with summaries for each chapter, numerous tables and several useful appendices.

Bequai, August. Computer Crime. D.C. Heath and Company (1978).

Though extremely opinionated and often oversimplified, this book is a fairly extensive review of the evidentiary problems surrounding computer crime as well as an expression of the difficulties involved in the actual prosecution of computer crime cases.

Carroll, John. Computer Security. Security World (1977).

A careful and detailed study of computer security, Carroll's work catalogues numerous cases (in Chapter 2) and in chapters on detection and surveillance (18) and record keeping and security (20) provides information of considerable use to the investigator.

Comer, Michael. Corporate Fraud. McGraw-Hill (1977).

Comer develops a sophisticated and extensive taxonomy of corporate fraud, and applies his analysis to computer crime as well (in Chapters 7 and 12). A very sophisticated work, well bolstered by examples, charts, lists, and tables.

Coughran, Edward. Computer Abuse and Criminal Law. Computer Center, University of California, San Diego (1976).

Though rambling and poorly indexed, Coughran's work on evidentiary and search and seizure problems involving computer crime is seminal, and is recreated in virtually every discussion of these topics. (Pages 29-61 are most helpful in this regard.) Coughran's collection of newspaper clippings, though arguably excessive, do provide good background to the general problem of computer crime.

Edelhertz, Herbert, et al. The Investigation of White-Collar Crime. LEAA (1977).

In addition to providing a detailed and extensive analysis of investigation of all sorts of white-collar crime, this widely cited text also contains a succinct summary of

computers in business data processing (pages 201-205) and computer crime investigation (pages 205-210).

Honeywell Information Systems, Computer Security and Privacy Symposium. Proceedings 1975, 1976, 1977, 1978, 1979. Honeywell Information Systems, Phoenix, Arizona.

Numerous of the presentations at the annual Honeywell Symposia have dealt with computer crime topics. Presentations vary considerably as to novelty, degree of technicality, and relevance to law-enforcement concerns. Each year tends to contain some relevant materials, however.

Krauss, Leonard, and Aileen MacGahan. Computer Fraud and Countermeasures. Prentice-Hall (1979).

Certainly the book of the year for computer investigation concerns, this is a thorough analysis of computer crime prevention, detection, and deterrence, mainly from an accounting point of view. This emphasis simply lends to considerable organization and documentation of the observations of the authors, and is not so technical as to put off the non-accountant. Chapter 1 addressing itself to a number of modalities of computer crime and Chapter 9 detailing a number of the most common computer crimes, both will repay careful study. Seventy pages of appendices contain a number of tables which would be useful for investigators trying to understand how a company or agency organizes its information and security vulnerabilities and controls as well.

Leibholz, Stephen, and Louis Wilson. Users' Guide to Computer Crime. Chilton Book Company (1974).

A good, brief mixture of a number of computer crime stories and a moderately sophisticated security analysis of the problems of computer crime.

Mair, William, Donald Wood, and Keagle Davis. Computer Control and Audit. The Institute of Internal Auditors, Altamonte Springs, Florida (1976).

A very sophisticated accountant's view of auditing computer systems. Numerous tables for analyzing a victim company's systems.

Martin, James. Security, Accuracy, and Privacy in Computer Systems. Prentice-Hall (1973).

Martin is a leader in instructional journalism relative to computers. Though occasional parts of his text are more sophisticated than most investigators will ever need, its scope, clarity, and wealth of illustrative detail makes it

a valuable resource. Extensive appendices cover the auditing and security functions overwhelmingly.

National Bureau of Standards. Federal Information Processing Standards Guidelines for Automatic Data Processing. Physical Security and Risk Management (FIPS PUB 31) (1974).

This is a classic government attempt to set up suggested procedures for computer security. Its brief format does not keep it from covering the field of security quite well.

National Bureau of Standards. Federal Information Processing Standards Guidelines for Documentation of Computer Programs and Automated Data Systems. Physical Security and Risk Management (FIPS PUB 38) (1976).

This manual attempts to set out in clear, organized fashion the different types of documentation a system should have and details the contents of these documents extensively. It is a useful supplement to the brief treatment of documentation found in this manual.

National Bureau of Standards. Approaches to Privacy and Security in Computer Systems. (NBS Special Publication 404) (1974).

This is a publication of proceedings of a seminar on privacy and security. It is most interesting to the investigator for its comments on security in general (pages 26-53).

Parker, Donn. Crime By Computer. Scribner's (1976).

Computer crime's number one student summarizes several of his more colorful cases in this book. Though targeted to a general readership it contains much analysis of the problem that has not been surpassed since, particularly his taxonomy as to the methods of computer crime, the extent of computer crime, ethics in the computing industry, and the consumers' stake in fighting computer crime.

Schabeck, Tim. Computer Crime Investigation Manual. Assets Protection (1979).

Though skimpy on details of computer crime cases, this book does meld a considerable amount of general information about investigation with some moderately clear information about how computers work and some valuable insights into the auditing considerations of computer crime investigation.

United States Senate, Committee on Government Operations. Problems Associated with Computer Technology in Federal Programs and Private Industry, Computer Abuses. (1976).

One of the opening salvos in the attempt to pass the Federal Computer Systems Protection Act, or viewed from another vantage, one of the reasons for the act, this report contains three General Accounting Office studies which suggest that there was not adequate security against computer crime involving government computers. Extensive background is contained in the some nearly 300 pages of appendices which constitute a virtual compendium of short studies of the computer crime problem.

United States Senate, Committee on Government Operations. Staff Study of Computer Security in Federal Programs. (1977).

This is an agency-by-agency analysis of computer use in the federal government and the vulnerabilities associated with that use. It also provides good background to the Federal Computer System Protection Act.

United States Senate, Committee on the Judiciary. Hearings on the Federal Computer Systems Protection Act. S.1766 (1979).

After the introduction of the Federal Computer Systems Protection Act, hearings were held enabling the computing, security, law enforcement, and business communities to provide input as to the strengths and weaknesses of the proposed legislation. This study contains considerable information as to the problems various spokespeople saw with the legislation and the general problems of computer crime.

Wagner, Charles. The CPA and Computer Fraud. Lexington Books (1979).

This book is valuable both in its general statistical analysis of the problems and its insight into the changing role of the auditor dealing with computer crime.

Whiteside, Thomas. Computer Capers. Crowell (1978).

This journalistic classic is the best popular treatment of computer crime. In its brief scope it manages to crystalize many of the major issues involved in the investigation and prosecution of computer crime.

Computer Newsletters

Three regular publications report recent computer crime cases and publish instructional material as to the investigation, auditing, and detection of computer crime.

These are:

"The Computer Security Newsletter." Produced by the Computer Security Institute, 5 Kane Industrial Drive, Hudson, MA 01749, sent to all institute members every other month. Membership costs $75 per year.

"Computer Fraud and Security Bulletin." A monthly sold by its publisher, Elsevier Journal Information Center, 52 Vanderbilt Ave, New York, NY 10017. Yearly subscription is $110.

"EDPACS." A monthly produced by Automation Training Center, Inc., 11250 Roger Bacon Drive, Suite 17, Reston, VA 22090. Yearly subscription is $48.

Law Journals

Computer/Law Journal Special Issue on Computer Crime, Computer/ Law Journal, 526 West 26th Street, Los Angeles, CA 90012.

An extensive analysis of legal issues involving the investigation and prosecution and defense of computer crime cases.

The Computer Security Journal, Computer Security Institute, 5 Kane Industrial Drive, Hudson, MA 01749.

The first issue is to be published in the middle of 1980. It will appear twice a year at an annual price of $35.

Fiction

The following books all involve computer crime in one form or another. Without passing judgment as to their artistic or technical merits, they are offered for the investigator seeking either busman's-holiday entertainment or an expanded consciousness of the potentialities of computer crimes.

Charbonneau, Louis. Intruder. Doubleday (1979).

Johannesson, Olof. The Tale of the Big Computer. Coward-McCann (1966).

Matthews, Clyde. The Ides of March Conspiracy. Arbor House (1979).

Ryan, Thomas. The Adolescence of P-1. MacMillan (1977).

Santesson, Hans. Crime Prevention in the Thirtieth Century. Walker and Company (1969).

Silverberg, Robert. Men and Machines. Meredith Press (1968).

Swigart, Rob. The Time Trip. Houghton Mifflin (1979).

APPENDIX 1

COMPUTER CRIME FIGHTERS ... GO TO BOOT CAMP AT FBI ACADEMY*

by Jay J. Becker

It was 10:30 at night, and Mohammed Ali was defending his title on TV. The FBI Academy bar was open, selling beer and wine, popcorn, and pool and ping-pong tables were available.

But George Monaco eschewed them all and sat huddled over a computer terminal, trying to land a lunar module without creating a crater.

In fact, George is an Assistant District Attorney from Chicago who had a total of three days exposure to computers in his life. Like 22 other prosecutors, George was in the midst of one of the nation's first courses designed to equip prosecutors to fight computer crime.

The lecturers at the week-long course left little doubt as to the need for such a course. The average loss from crimes involving computers is $450,000. This contrasts drastically with average losses of $9,000 from bank robbery and $19,000 for embezzlement.

Though the incidence of computer crimes is still small in absolute numbers (144 cases reported to the police and 708 reported to any source, according to FBI statistics), all indicators point to the likelihood that the number of incidents will increase substantially in the future.

Bill Colvin, an instructor in the FBI Academy's Economic and Financial Crimes Training Unit, projected a growth of computers in use in our country from 150,000 at present to 500,000 in the 1980s. James Barko, chief of the unit, draws the conclusion: "As more people automate, more financial records will be put on computers. People, including criminals, simply go where the money is."

Additionally, students of computer crime predict changes in the types of computer criminals in the years ahead. Computer criminal profiles compiled by Donn Parker of the Stanford Research Institute indicate that most of those accused of computer crime are amateurs and first offenders. Often, Parker says, they are motivated more by the challenge of beating the system than the monetary gain. Although this analysis is undermined by t.e loss figures reported above, it highlights

*Reprinted with permission from Security World, September, 1978, pp. 30-31.

the possibility for a change for the worse in the nature of the computer criminal. Not only are more people becoming knowledgeable in computing, but individuals who present a greater threat of criminal behavior are gaining this expertise. Prisoners in numerous institutions are learning computer programming, sometimes from convicted computer criminals. Although little evidence has surfaced to indicate that organized crime is heavily involved in computerized crime, Barko's statement that people go where the money is holds true for organized crime. Thus, both Parker and the lecturers at the FBI course stressed the fear that organized crime involvement in computer crime is very likely to increase.

Perhaps the most telling aspect of the computer crime problem as it relates to prosecutors was the statistic derived by instructor Colvin. "One percent of all computer crimes is detected," he informed them. And approximately 7 percent of the crimes that are detected are reported to the police. Moreover, in those cases brought for prosecution, only 1 out of 33 results in a jail sentence for the accused. Simple calculation leads to the chilling conclusion that only 1 out of every 22,000 computer criminals is going to go to jail.

This statistic makes it clear that prosecution must rise to meet the challenge. Barko explained that part of the reason for the FBI sponsorship of this course was: "We train our agents in computer crime--what if they go to a lawyer and he doesn't know what it all means? Maybe he can prosecute the case, but I don't know if he can win it." Many of the prosecutors who attended the course shared Barko's fear that without training in the basics of computers and programming, they could not adequately handle the cases that came to them for prosecution. Many had already faced computer crime prosecutions and had experienced difficulty with these cases.

Thus it was natural that the Economic Crime Project, a project of the National District Attorneys Association, should approach the FBI Academy and request that it set up the computer crime prosecution course.

The stage was set on February 12th for prosecutors from throughout the country to gather for the long bus ride from Washington, D.C., to Quantico, VA, some 40 miles away.

Two prosecutors sat on the bus and wondered about the experience that lay ahead. "Do you know anything about computers?" one asked, smoking nervously. "A little," the other replied. "I had a course while I was in law school, but I am afraid it may be over my head, and I will be the only prosecutor in the room who doesn't already know a lot about computers."

His fears were neither justified nor unique. A test given to the prosecutors at the beginning of the course to ascertain their computer backgrounds indicated that many of the attorneys did not know the use of magnetic tape in a computer system, the purpose for which COBOL is usually used, the configuration of an IBM punch card, or the definition of batch processing.

In the middle of one class, a student expressed what many were probably feeling. When asked if the "S" which abbreviated for his first name on the teacher's seating chart stood for Steven, he replied, "No, it's for stupid."

The FBI staff was more than eager to give these prosecutors an awareness of computers and a comfort in dealing with them that few anticipated.

Combining the expectation of hard work, friendly patience, virtually complete access to the FBI computer, and a variety of motivational techniques, the staff proceeded with efficiency to create a core of computer crime cognoscenti. There was a heavy dose of homework. In four days, the prosecutors were expected to read half of a text on computer fundamentals. Evenings found the deputies recreating college life, buddying up to study.

In the 8:00 a.m. to 5:00 p.m. daily classes, the students went through a thorough grounding in the basics of computers. They learned computer vocabulary, the nature of a punch card, how a computer works, input and output devices, and flowcharting. This was preliminary to a major segment of the course devoted to programming. By the second day, the men and women had learned enough RPG II to begin to work on their first practical problem, a simple listing program. The class gathered in the FBI's computer center, many of them sitting down to keypunch for the first time.

Two precocious students went to the computer terminal and read the instructions. Bob Sussman, head of the Economic Crime Project and organizer of the course, nervously paced, and kept his distance as the students carefully, and not without their own misgivings, continued. They tried several times, referred to the manual, and speculated why they couldn't get the programs they had keypunched to compile.

Finally, the two students called on Ken Lewis, one of the course instructors. Unperturbed, he told them where they had gone wrong. Later, Lewis explained the importance of access to the FBI computer: "Hands-on experience is a big part of this course," he said. "Some courses won't let you get near a computer, but all we have our computer for is to teach students how it works. Students worry about damaging the computer, not knowing how hard it is to actually do any damage."

Access to the computer became a greater advantage as the students were able to use the computer night or day for the three remaining course days. The problems the students were given to solve proved highly motivating, as the lawyers' standards of performance ran up against the perfectionism of the computer. Seeing a simple program generate pages of diagnostic messages caused many a student to do it over until he got it right.

Perhaps the high point of the course came on the fourth day when the prosecutors were called upon to apply everything they had learned about computers, programming, and computer fraud to a practical problem. In the course of this three-hour exercise, the class was taught COBOL, given a basic course in accounting, shown a small stack of computer printouts, and told to find the crime that these printouts evidenced.

Each of the groups succeeded in detecting that a crime had been committed, although explaining how proved more difficult. Nonetheless, and perhaps more significantly, the class members were able to follow Professor Colvin's explanation of the programming involved. One had little doubt that the prosecutors could have understood an investigator explaining what had gone wrong equally well, and have little more trouble explaining it to a jury.

On Friday afternoon, the last class had been completed and the goodbyes said. Three students were at work in the computer room. Casually, they turned on the machine and worked on their program, looking for all the world as though they were experienced operators.

The lawyers left Quantico confident they could deal with the computer. They no longer saw it as a mysterious or intractable adversary. Participants questioned about the advantages of their training stressed the usefulness of the information they had gained as to how both computers and computing centers work. The prosecutor from Washington, D.C., summed it up well: "When an expert talks to me about computers now, I can relate what he is saying to my own experience."

With this knowledge comes an ability to communicate more directly and meaningfully with the computer experts that are often necessary at the various stages in the prosecution of a computer crime. As Jim Barko put it: "It is not enough to learn what the computer expert means at the same time that the jury is learning it. To actively prosecute a case, a prosecutor must go into the court with a much more thorough grasp of the subject matter.

No one pretended that this introduction to computers made the prosecutors instant experts. Mr. Barko broke the news to

the participants: "A week from now, few of you will be able to program anything in RPG II, let alone in COBOL. However, if you understand that the computer is a demanding and precise beast, and you remember that you have the ability to learn how to program it, our course will have been a success."

* * * *

APPENDIX 2

National Center for Computer Crime Data

Jay Becker, Director

320 W. Temple St. Rm. 540
L.A. Ca. 90012
(213) 974-3955

INFORMATION SHEET

1. WHAT IS THE NATIONAL CENTER FOR COMPUTER CRIME DATA?

   The National Center for Computer Crime Data is a collection of resource materials designed to facilitate the prosecution and investigation of computer crimes. (Computer crime is defined by the Center in as broad a way as possible, and includes all crime perpetrated through the use of computers and all crimes where damage is done to computers.)

2. WHY WAS IT CREATED?

   There is a growing need for rapid and informed response to the technological questions posed by computer crime. Many of these questions are beyond the expertise of the local police officer, prosecutor, or court. We expect that more and more of these technical questions can be answered by the National Center for Computer Crime Data.

3. WHAT MATERIALS DOES THE CENTER CONTAIN?

   The National Center for Computer Crime Data consists of a variety of resources:

   Legal work products: Search warrants, memoranda of points and authorities, criminal and civil complaints, trial briefs, legal periodical articles and texts.

   Legislation relevant to the definition of, and sanctions against, computer crime, and to related issues such as EFTS, privacy and the like.

   Case summaries indicating the types of crime already known to have been committed and the modus operandi of these crimes.

   Scholarly materials dealing with general themes relating to computer crime, including statistical studies of the incidence and costs of computer crime, and analyses of computer crime problems from ethical, security, accounting, and computer industry viewpoints.

   Index to current research (ICR): A collection of summaries of ongoing research in computer crime.

   Knowledge net: Additionally, the National Center for Computer Crime Data maintains a "knowledge net" and an experts index. Both prosecutors who have tried computer crime cases and experts in areas relating to computer crime are listed in the "knowledge net." The purpose of the "knowledge net" and the experts index is to formalize an "old boy" (or, to be more timely, an "old person") network which will enable callers to find local prosecutors and others experts they can consult with on computer crime problems.

4. HOW DOES IT WORK?

   The Center exists specifically to collect and disseminate information, and that is possible only if members of the public, prosecutors' offices, business, computer, accounting, and security industries contact us. If you have documents or information as outlined above, please write or call us for help. For further information, contact Jay Becker.

APPENDIX 3

CHARACTERISTICS AND RESPONSIBILITIES OF EDP FUNCTIONS*

FUNCTIONAL GROUPINGS	FUNCTIONS INCLUDED	GROUP CHARACTERISTICS	RESPONSIBILITIES
INFORMATION PROCESSING FUNCTIONS	Operation of computer and related equipment Data conversion Library Control group	Highly repetitive work loads predictable and subject to scheduling Operations routine require supervision Instructions necessary Operations subject to performance measurement Visible results for users Quality of controls, readily determinable	Achieve efficiency for group as a whole Maintain committed schedules High level of accuracy for data processed Maintain quality consciousness for group as a whole
PROJECT FUNCTIONS	Systems development Procedures and forms Quantitative analysis Programming	Only nominally repetitive Long duration Projects with structured activities for visible interim results High level of interpersonal skills Numeric orientation (quantitative analysis) Systems analysis skills necessary	Understand objectives, responsibilities and functioning of user organization Improve effectiveness of user through application of EDP processing
TECHNICAL SERVICES FUNCTIONS	Equipment selection Software and operating system selection Program maintenance Quality assurance	Highly technical Results may have low user visibility	Technical support to operating and project functions Improve efficiency and effectiveness of operating and project functions Development and maintenance of standards for computer operations Monitor compliance with standards

*From Computer Control and Audit by William Mair, Copyright 1978 by the Institute of Internal Auditors, Inc., 249 Maitland Avenue, Altamonte Springs, Florida 32701. Reprinted with permission.

APPENDIX 4

Table D.29. Specimen Checklists for Auditors*

The following checklists are based on actual questionnaires that are in effective use in several different organizations.

Checklists for accuracy control, control of terminal operators, physical theft protection, file construction software features, and control of classified documents are not included as these are dealt with at length in the earlier tables.

1. CONTROLS ON PERSONNEL	Not Applicable	Scope of Review & Period Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
Are responsibilities divided so that fraud cannot be carried out without collusion?						
Are departments and close associates separated so as to minimize the likelihood of collusion?						
Are personnel handling the corporation's assets entirely separate from personnel involved in data processing?						
Are background checks performed on all new hires?						
Are critical personnel bonded?						
Do managers know their subordinates sufficiently well to detect disgruntled employees, or employees who are in trouble; who might be a threat to the installation?						
Can employees who constitute a threat be transferred or dismissed immediately?						
Are critical jobs rotated periodically?						
Are employees cross-trained so that if any critical employee becomes unable to do his job another can immediately take it over?						
Is the level of training sufficiently high?						
Is there a continuing education program?.						
Is security included in this program?						
Do all personnel take security seriously?						
Are casual practices—such as leaving classified documents unlocked—to be found?						
Is a "clean desk" policy enforced?						
Controls on programmers—See Table D.19						

* From James Martin, Security, Accuracy, and Privacy in Computer Systems (Prentice-Hall Publishing Company, 1974) Reproduced with permission.

Table D.29. (continued)

2. SENSITIVE PROGRAMS	Not Applicable	Scope of Review %-Period-Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
Definition of a "sensitive" program: A sensitive program is one in which a programmer can, by changing program instructions *only*, misappropriate company assets and conceal the act even though adequate administrative processing controls are in place. They are the programs in the system where important internal control tests are made. The more sensitive areas have been identified as Payroll, Accounts Payable, Fixed Assets, Purchasing, and Inventory Control. (Note: Although there may be many programs in a given system, such as Accounts Payable, only a small number may contain internal control tests. These should be identified as the sensitive programs. The other programs should not be identified as such. To identify all programs in Payroll, Accounts Payable, etc, as sensitive defeats the purpose of the control which is to establish reasonable protection from programming fraud without burdening the location. Controls over unnecessary programs make the controls costly and less effective.)						
1. Is there a control list for sensitive programs identifying the responsible programmer and his manager?						
2. Is there adequate separation of maintenance responsibility for sensitive programs between programmers?						
3. Are programs and documentation stored in a secure location to prevent unauthorized access? Each storage area should maintain a log that shows the program requestor's name, date, and authorization reference.						
4. Is unauthorized patching and changing of sensitive programs prevented, or could a programmer or operator bypass the safeguards?						
5. Does an independent party review all requests for updates to sensitive programs, and advise management of questionable changes?						
6. Is there controlled maintenance of a history of assembled programs? Local management discretion should be used on the number of documented changes to be maintained, since frequency of change will vary by program.						
7. Are there sufficiently frequent unannounced periodic audits of program changes for authorization and documentation?						

Table D.29. (continued)

4. INPUT/OUTPUT CONTROLS	Not Applicable	Scope of Review %-Period-Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
1. What controls exist for input of sensitive data from point of origin?						
2. What controls exist for the distribution of output to designated areas?						
3. Are controls established for point of origin review of rejected sensitive transactions?						
4. What type of controls are established for correcting errors in input/output with the point of origin?						
5. Are predetermined totals or item counts maintained within the DP operation and compared with keypunch, unit record, or computer output prior to being sent to the customers? The person maintaining the controls should not be involved in processing the data.						
6. Keypunching–are all important data fields subject to mechanical verification by operators using verifier machines?						
7. Are limit checks included in appropriate programs? On input? On output? Is appropriate action taken when limit checks are violated?						
8. Review the controls listed in Tables D.8 and D.12. Should any of these be added to the controls currently in existence?						
9. Is appropriate segregation of duties in effect for persons who handle sensitive data?						
10. Are data control personnel provided with schedules listing the dates that programs will be run, the due in and due out times, the dates for customers providing input data and the date for distribution of output. Schedulers should monitor the flow of work. *Note:* This will facilitate the flow of work to the computer and reduce idle time awaiting input.						
11. Is the backlog of jobs reasonable? Review for excessive delays.						
12. Is rerun time due to error by operator, programmer, or other Information Systems personnel segregated and charged to department overhead?						

Table D.29. (continued)

4. INPUT/OUTPUT CONTROLS (continued)	Not Applicable	Scope of Review %-Period-Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
13. Has responsibility been established for following up all input errors to ensure that they are properly corrected and returned for processing?						
14. Are the exceptions (or significant events) logged by Machine Operators reviewed by management and is action taken?						
15. Are reasons determined and corrective action taken for rerun hours (machine-operator-input-program)?						
16. Are all significant deviations from targets established for "hands on" time rerun checked?						
17. What is done about low utilization machines and overload situations?						
18. To test the system's validation controls, the auditor should feed in invalid transactions and see what the system does with them.						

Table D.29. (continued)

6. COMPUTER CENTER OPERATIONS	Not Applicable	Scope of Review %-Period-Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
1. Have computer center operating procedures been written?						
(a) Are they sufficiently descriptive in detail to guide the organization and operation?						
(b) Are they kept up-to-date?						
(c) Does the computer center operate independent of the programming area?						
2. Do operators' instructions for running each job include:						
(a) Identification of all machine components used and purpose?						
(b) Identification of all input/output forms?						
(c) Explanation of purpose of run?						
(d) Detailed input and output disposition instructions?						
(e) Identification of all possible programmed halts and prescribed restart instructions?						
3. Is an operating log maintained to record any significant events and action taken by the operator? (Proper recording would indicate whether operators were following instructions for halts in programs, etc.)						
4. Is the operator log inspected daily by management?						
5. Are the pages of the operator log prenumbered, or is some other method used to ensure total accountability?						
6. Are data control center personnel and operators' assignments rotated? (This not only aids in cross-training, it helps avoid fraudulent manipulation of jobs.)						
7. Are logs maintained to record the CPU meter readings (for both customer and CE meters) at the start and end of each shift? Are variances explained?						
8. Are CE maintenance logs kept current? (These logs are especially important when recording reruns caused by machine failures. This time should be claimed against any additional billable time.)						
9. Are trouble reports prepared when processing is interrupted because of operator or program(mer) error or machine failure? (The reports should indicate what caused the problem and what action was taken.)						
10. Are computer room personnel the only individuals allowed to operate the machines?						

Table D.29. (continued)

6. COMPUTER CENTER OPERATIONS (continued)	Not Applicable	Scope of Review %-Period-Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
11. If programmers operate the machine, is this time controlled? (a) Are programmers required to obtain written permission from their department manager for all "hands on" time? (b) Is management able to determine whether programmers are making excessive tests and assemblies due to poor programming techniques? Is control adequate? (c) Are targets for reasonable "hands on" time rerun due to operator or programmer error established?						
12. Are operators denied access to program flow charts, source decks, program listings, etc.? (The operator does not need access to these items to perform his duties. Consequently these items should be maintained outside of the computer room to prevent changes to programs or operation by computer operators.)						
13. Do programmers test their programs with "live data"? Are there procedures in effect to control this?						
14. Are adequate safeguards exercised to ensure that only authorized persons are permitted in computer or machine areas? Are these safeguards effective in practice?						
15. Do operators know what to do when an unauthorized person does come into the machine room and is intent upon stealing something or doing harm?						
16. Do the operators know what to do in the event of fire or other emergency?						
17. Is there a surveilling escort for all visitors?						
18. Are demonstrations controlled?						
19. Are computer operating staff adequately screened before hiring?						
20. Are all computer runs supported by a work request or other written authorizations? (This includes scheduled and nonscheduled production assemblies and tests.)						
21. Are the above approved by management? If not, are there other controls to ensure that *all* computer runs are justified?						

Table D.29. (continued)

6. COMPUTER CENTER OPERATIONS (continued)	Not Applicable	Scope of Review %-Period-Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
22. Are there provisions for scheduling of jobs on the system? These provisions would include: (a) Due dates of input and output (b) Records covering delays in receipt of input; processing of data; delivery of output (c) Establishment and adherence to priorities						
23. Is all input data accompanied by control totals, or other control information (such as number of cards, reels of tape and records per tape, etc.)?						
24. Are control totals produced independently by the tape/disk/drum loading program?						
25. Are input, load, and output totals reconciled after processing?						
26. Input errors; Are the users provided with data error listings that report on the accuracy of their input data?						
27. Are there procedures to extend document control to such items as blank checks, stock certificates, etc.?						
28. Is adequate control maintained over the input and output data? (Trace the flow of operational data through the computer and/or machine room.)						
29. Are system utilization and usage reports distributed to management for their review of: (a) Operating system reporting (b) Productive time (c) Program test and assembly (d) Operating system generation (Sysgen) (e) CE maintenance time (f) Programmer "hands on" time (g) Demonstration time (h) Rerun time (i) Idle time (j) Power off time (k) Other (other location backup, etc.)						

Table D.29. (continued)

6. COMPUTER CENTER OPERATIONS (continued)	Not Applicable	Scope of Review %-Period-Quantity	Satisfactory	Unsatisfactory	Scheduled for Implementation On	Workpaper Reference
30. Is "productive time" broken down into scheduled and nonscheduled production? (Periodic comparison of productive to nonproductive time and scheduled to nonscheduled production is necessary to ensure reasonability. The Utilization Reports are also needed to evaluate system effectiveness and profitability; help plan manpower and hardware work loads; provide a basis for scheduling new job capacity.)						
31. Are "turn-around" (time on and time off the system) reports distributed for Management review?						
32. Are procedures for billing charges for computer usage and/or cost allocations, if applicable, based upon operating records?						
(a) Can departmental charges be reconciled back to the usage/utilization reports or turn-around reports?						
(b) Is rerun time caused by programmer, operator, systems personnel or machine error segregated and charged to overhead rather than to the using department?						
(c) If using departments are not charged for computer time, is there a procedure to ascertain the need for regularly scheduled production jobs?						

APPENDIX 5

IN THE

MUNICIPAL COURT FOR THE SAN JOSE-MILPITAS JUDICIAL DISTRICT,

COUNTY OF SANTA CLARA, STATE OF CALIFORNIA.

SEARCH WARRANT

THE PEOPLE OF THE STATE OF CALIFORNIA

To any Sheriff, Constable, Marshal, Policeman, or Peace Officer in the County of Santa Clara:

Proof, by affidavit, having been made before me this day by TERENCE GREEN that there is just, probable and reasonable cause for believing that: evidence of the commission of a felony, to wit: Theft of Trade Secrets, described in Section 499c of the Calif. Penal Code, more particularly described below, will be located where described below.

You are therefore commanded, in the daytime or nighttime, to make immediate search of the University Computing Corp., 260 Sheridan Avenue, Palo Alto; the residences of _____ at ____, Menlo Park, and at _____ Menlo Park; a 1966 Porsche, Calif. Lic. _____, registered to said _____ and the person of _____.

located at the addresses noted above, County of Santa Clara, State of California, for the personal property described as follows: 1) Key punch computer cards, punched with the Information Systems Design remote plotting programs; 2) Computer printout sheets with printouts of Information Systems Design remote plotting programs; and 3) Computer memory bank or other data storage devices magnetically imprinted with Information Systems Design remote, plotting computer programs;
and if you find the same or any part thereof, to hold such property in your possession under Calif. Penal Code Section 1536.

Given under my hand this 19th day of February, 1971.

/s/
Judge of the Municipal Court

WPH:nas

IN THE

MUNICIPAL COURT FOR THE SAN JOSE-MILPITAS JUDICIAL DISTRICT

COUNTY OF SANTA CLARA, STATE OF CALIFORNIA

STATE OF CALIFORNIA)
) ss.
COUNTY OF SANTA CLARA)

AFFIDAVIT IN SUPPORT
OF SEARCH WARRANT

Personally appeared before me this 19th day of February 19 71, TERENCE GREEN who, on oath, makes complaint, and deposes and says that there is just, probable, and reasonable cause to believe, and that he does believe, that there is now in the possession of _____ and UNIVERSITY COMPUTING CORPORATION, on the premises located at University Computing Corp., 260 Sheridan Avenue, Palo Alto, Calif., and residences of _____ at _____, Menlo Park, Calif., and _____, Menlo Park, California, which premises consist of: University Computing Corp., a business, and said _____ residences occupied by said _____, a 1966 Porsche, Calif. Lic. _____, registered to _____ and the person of _____ personal property described as follows:

1) Key punch computer cards, punched with the Information Systems Design remote plotting programs;

2) Computer printout sheets with printouts of Information Systems Design remote plotting programs; and

3) Computer memory bank or other data storage devices magnetically imprinted with Information Systems Design remote plotting computer program.

Affiant, Terence Green, is a Sergeant of Police attached to the Fraud Detail of the Oakland Police Department and is engaged in the apprehension of persons engaged in the theft of trade secrets and commercial property.

Affiant was advised on February 4, 1971, by Mr. George Steeley, President of Information Systems Design, a corporation with offices at 7817 Oakport Road, Oakland, that he had discovered a set of key

punch cards at a terminal electrically connected to a computer owned and operated by his corporation, which terminal is located on the premises of the Shell Corporation in Emeryville, Alameda County. That his personal examination indicated that the key punch cards relate exclusively to a program on the computer of his corporation which program gave the computer the capability of producing remote plotting. That the remote plotting capability is a program which was designed and developed by his corporation and was used and regarded by them as a trade secret. That the value of this program in the data processing industry is estimated by him at $15,000.00. That his examination of the key punch cards shows that the computer was implemented by use of an access code to that particular program, which code was regarded by his corporation as confidential, and was not released by them except to persons authorized by them. Further that the production of the program was further initiated through use of the site number assigned to the Shell Corporation facilities. That Mr. Steeley has confirmed with officers of the Shell Corporation that the implementation was not made by them or at their request. This affiant has further contacted Mr. Jerry Helmuth, special agent with the Pacific Telephone Corporation and is apprised by Mr. Helmuth that a telephone call was made to the telephone number then exclusively leased to the Information Systems Design computer from a number then exclusively leased to the University Computing Corporation at 260 Sheridan Avenue in the City of Palo Alto. That that call lasted 11 minutes and 32 seconds. That Mr. Keith Marcelius, an

employee of Information Systems Design, has examined their computer and has advised affiant that the computer was used for the purpose of printing the confidential program at the same time that the telephone call was placed from the University Computing Corporation.

That Mr. Marcelius, who is employed by Information Systems Design as an expert in the functioning and operation of the UNIVAC 1108 computer, has advised your affiant that the confidential remote plotting program would have been reproduced at the terminal which he personally knows to be located at the premises of University Computing Corporation.

Affiant is further advised by Mr. Keith Marcelius that, prior to the 19th of January, 1971, and thereafter, a _____ ____was employed by University Computing Corporation. Mr. Marcelius has further advised affiant that _____ had been a representative of University Computing Corporation in utilizing the computer installation to the Shell facilities. The use of which installation was shared with Information Systems Design. That affiant is further advised that _____ had access to both the Shell site number and the access code to the Information Systems Design confidential program, but that he had not been authorized to utilize the latter.

Mr. Marcelius further advised affiant that the program, the property of Information Systems Design, could now be held in various forms: 1) In the form of key punch computer cards as were discovered at the Shell facilities; and/or 2) in the form of computer printout sheets; and/or 3) could exist in an intangible form as a program in a computer, which program, consisting of a series of

accessible electrical and/or magnetic impulses, could be disclosed only through interrogation of such computer and any data storage device. That in either key punch card or computer printout sheet form this program would be readily moveable.

Mr. James Verner, Manager of Customer Support for Information Systems Design, advised affiant that he was personally acquainted with _____, that to his personal knowledge _____ knew of the existence of the Information Systems Design, and further that ____ ____ had represented generally that he was able to get into the Information Systems Design computer.

Your affiant has contacted the Department of Motor Vehicles of California and from them has been advised that _____ is the registered owner of a 1966 Porsche, license number _____ which vehicle is currently registered to him at _____ in the City of Menlo Park. Affiant is further advised by Mr. Steeley that _____ current address is _____ in the City of Menlo Park.

Mr. Keith Marcelius has furnished affiant with a series of key punch computer cards punched with the Inforamtion Systems Design remote plotting programs and a printout sheet with a printout of the Information Systems Design remote plotting programs and is accompanied by Mr. Keith Marcelius, an expert in the use of said cards, printouts, and the manner in which magnetic information is stored in computers, as well as the Information Systems Design remote plotting program.

Affiant believes that the personal property first above described will constitute evidence of the commission of a felony, to wit: Theft of Trade Secrets, as described in Section 499c of the Calif. Penal Code, and that said evidence will be in the possession of University Computing Corporation at its address and business first above described, and in the possession of _____ at his residences above described and in a 1966 Porsche automobile above described.

Affiant desires to search at night because he has ascertained that said University Computing Corporation operates its business both day and night, and it is now approximately 5:00 pm, and it may well be dark by the time affiant can obtain a signature of the magistrate to this warrant and conduct the aforementioned search.

Further, affiant has been informed by Mr. Keith Marcelius that said magnetic impulses in the computer can be altered or destroyed in a matter of a few minutes.

That based upon the above facts, your affiant prays that a Search Warrant be issued with respect to the above location for the seizure of said property, and that the same be held under California Penal Code Section 1536 and disposed of according to law.

/s/
TERENCE GREEN

WPH:nas

Subscribed and sworn to before
me this 19th day of February, 1971.

/s/
Judge of the Municipal Court

IN THE MUNICIPAL COURT FOR THE SAN JOSE-MILPITAS JUDICIAL DISTRICT
COUNTY OF SANTA CLARA, STATE OF CALIFORNIA

PROPERTY RECEIPT

Inventory of items taken pursuant to Search Warrant issued by the Honorable Louis C. Doll, Judge of the Municipal Court, upon the affidavit of Sergeant Terence Green, Oakland Police Department, on February 19, 1971.

1. Total directory of all files on Fastrand at University Computer Corp., hereinafter UCC, at 260 Sheridan Avenue, Palo Alto, California, consisting of continuous print-out sheets.

2. Abbreviated as to description directory of files of Fastrand at UCC, at same address, as of 0730 19 February 1971, consisting of continuous print-out sheets.

3. Abbreviated as to description directory of files "dumped" from Fastrand to paper at 2300 hours, 19 February 1971.

4. Nine (9) tapes, the result and product of the "dumping", item 3, supra.

5. List of nineteen (19) tapes of UCC, the property of UCC, assigned by UCC to _____ for him to use on UCC business.

6. Program listing of a computer run, 2 February 1971, from 12:05:08, sequance #180.

7. Nineteen tapes, each in a plastic container, referred to in item 5, supra.

8. White binder, consisting of a number of listings of computer runs, labeled "Aerojet-General _____, binder approximately 12" x 15" x 1".

9. Olive desk file folder, metal mounts, containing:
   a) six handwritten pages, paper clipped, labelled ISD Message Format
   b) ISD Univac 1108 Users Guide 1 April 1969, bound
   c) ISD Univac 1108 Users Guide 1 April 1969, two copies, xeroxed, unbound. (approximately 70 pages each)

10. A manila file folder, labelled "Plot Packages" containing:
    a) CALCOMP Operation Manual Model 611 Offline Dataphone ... Part No. 10037-901-001-0, datad November 1969, blue binder
    b) CALCOMP Operation Manual for Model 663 Plotter, dtd March 1970, blue binder
    c) California Computer Products, Inc. Manual, Programming Calcomp Pen Plotters, dtd June 1968, labelled _____
    d) CII Applications Software, Pub No 585b, July 1969, yellow softbound, labelled _____.

11. Olive desk file folder, metal mounts, labelled PLOTTING.

12. Manila file folder, labelled AEROJET-GENERAL, containing
    a) 35 reproduced pages
    b) 3 handwritten pages

13. Manila file folder, labelled AEROJET-CALCOMP, containing
    a) five xeroxed pages labelled ISD
    b) three unlabelled xerox pages
    c) seven handwritten sheets

IN THE MUNICIPAL COURT FOR THE SAN JOSE-MILPITAS JUDICIAL DISTRICT
COUNTY OF SANTA CLARA, STATE OF CALIFORNIA

PROPERTY RECEIPT
Continuation

14. Mottled grey binder, consisting of a number of listings of computer runs, labelled ISD, approximately 12" x 15" x 1/2".

////////////////////////// Nothing Follows //////////////////////////////////

Received, pursuant to Property Security Agreement made this date with University Computer, Corp.

/s/

APPENDIX 6

PROGRAMMED FOR CRIME*
by Jay Becker

A computer's ability to store vast amounts or information makes it a prime target for criminals. Yet detecting, prosecuting and defending computer criminals require specialized knowledge of computer technology. As such, the increase in computer crimes and the dirth of case law in this area are creating nightmares for the courts.

It was a sign of the times. In a recent issue of Computerworld was a feature called "Crime Wrap-up." The article, which occupied a prominent spot in a major computer industry periodical, contained the news that Michigan had become the fifth state to pass legislation concerning computer crime. Right beneath it were separate stories of three different computer crime cases, one involving an acquittal, one a plea and one an indictment. Beneath these stories, at the bottom of the page, was an advertisement for a national management consultant specializing in computer security. "There's always the chance something or someone can 'get to' your computer," the ad warned investigators in computers and computer crime. The Law Enforcement Assistance Administration (LEAA) is getting ready to award a $400,000 contract for additional training of prosecutors and investigators in computer crime. Here in California, as in five other states, computer crime legislation is pending.

Thus, it seems likely that computer crime problems will arise more and more frequently in the criminal trial of the future.

Although computer crime is not the only area where lawyers must try to adapt precybernetic laws to the realities of current technology, it is of growing significance in what has become the most information-oriented society ever to exist. Whether it is computer copyright, software taxation, issues of liability when computers are involved in industrial accidents, or clauses in purchase contracts for comuter hardware, the law

---

*Los Angeles Lawyer, November, 1979, pp. 16-31. Portions of this article are reprinted with permission of the L.A. County Bar Association. Copyright 1979. All rights reserved. Jay Becker writes frequently about computer crime from his vantage as director of the National Center for Computer Crime Data, a clearinghouse for information about computer crime investigation and prosecution. He is head of the Los Angeles County District Attorney's Antitrust Section.

is being forced to recognize that the widespread use of computers is causing changes in our society so different in degree as to be almost different in kind.

Though some would suggest that the computer is no more than a big adding machine, it is impossible to look at the phenomenon of computer crime without considering the varied effects of computers on our legal consciousness.

On a physical level, the computer staggers us by its ability to concentrate and manipulate enormous quantities. Information, money, complex mathematical equations, or repetitive tasks all fit within its grasp.

On an intellectual level, computers have changed our vocabularies, and perhaps more importantly, our concepts of how things get done. Whether we think about a word like deprogramming or we ask someone for feedback, systems and information science theories have caused us to talk and think in new ways. For instance, to date, the law has no consistent answer to the demand to redefine property in view of the value of information in the age of the computer.

Finally, there is a third kind of reaction--a response on a mythical level--to the incursion of computers into our lives. This reaction does not affect the way we think but shapes the stories we tell ourselves when we don't know what to think. Such unthinking reactions are responsible for some of the more colorful and interesting aspects of social behavior, as well as some that are critically important. For example, few criminal lawyers would deny the power of sexist mythology in the area of rape. Unthought prejudices about men, women, sex, and other vague and farreaching ideas color, if not dictate, decisions in many a rape jury. In the same way, unarticulated feelings about computers affect the whole realm of computer crime. As we will see, publicity both creates and caters to computer myths, and computer crime sentencing often reflects them.

Inexplicably, none of these dramatic changes has brought forth a flood of legal literature about trials of computer crimes,[1] and even less guidance is available in case law.

Consequently, much of the information presented here is anecdotal, representing the responses to a survey of attorneys who tried (or plea-bargained) computer crime cases,[2] investigators who contacted the National Center for Computer Crime Data (NCCCD),[3] and case histories already in the NCCCD's files.

Much as I would like to generalize from these specifics, all but the broadest generalizations seem premature.

SEARCH AND SEIZURE

One need only consider the requirements for a search warrant in light of the complexity of computer technology to begin to imagine the search and seizure issues inherent in computer crimes. The enormity and complexity of the "scene of the crime" where computers are involved is demonstrated by the litigation involving Equity Funding Corporation of America. There, thousands of fictitious insurance policies had been created and existed somewhere within a computer memory. At the same time, this computer was processing hundreds of thousands of valid insurance policies. According to Carl Pabst, a partner in the accounting firm of Touche-Ross, appointed by the trustee in the Equity Funding bankruptcy proceedings, it was impossible to maintain adequate security over the computer site while allowing the business to continue to function.

Both in drafting a warrant and serving it, problems can be severe. Simply describing what is to be taken and how it can be recognized, so that a magistrate will find the particularity requirements of Penal Code Sections 1525 and 1529 satisfied, is a bit more difficult when it is premised on an understanding of computer language, and perhaps of computer operations as well. For instance, in Alameda County, in the case of People v. Ward, Municipal Court Judge Lewis Doll was asked to sign a search warrant authorizing the seizure of, among other things, "computer memory bank or other data storage devices magnetically imprinted with Information Systems Design (ISD) remote plotting computer programs." Ward was believed to have stolen a program from ISD and made it available to University Computing Co., one of ISD's competitors. Alameda County Deputy District Attorney Don Ingraham attempted to explain the specifics of Ward's theft, alleging that the stolen program was valuable because it was capable of "producing remote plotting." Then, remote plotting had to be explained and the fact that it was designed and developed by ISD. This was a ticklish task since California law is still unclear as to whether stealing the information in a program is a crime. (See discussion of this aspect of the Ward case below.)

> It is impossible to look at computer crime without considering the varied effects of computers on our legal consciousness.

Another difficult problem was that the prosecutor did not know in what form the stolen program might be found at the scene of the search. The search warrant affidavit indicated that it might be found in the form of computer printout sheets, or in an intangible form within the computer. To locate the material to be seized, an expert from the victim company was to accompany the officers serving the warrant.

For the attorney drafting such a warrant, great care must be taken to learn enough about the computer operation involved to describe adequately those aspects which are relevant. Additionally, they must be described clearly enough to be understood by the magistrate. It goes without saying that, without a comparable knowledge on the part of the defense attorney, he or she will be in no position to contest the adequacy of description of many items contained in the warrant.

There is considerable value in having an expert available when the warrant is served in those cases where neither the attorney nor the investigator serving the warrant has enough knowledge of the computer system to perform a search intelligently and completely. It may be the case that only the expert has a sufficient background in programming to query the computer, locate the relevant information stored in the computer, retrieve it, and do all this in such a manner that no harm is done to the operation of the computer system. Yet, until August 1979, it was unclear under California law whether an expert can be taken to the scene.[4]

Though search and seizure issues have been raised in various computer cases,[5] none has turned up in the cases reported to the National Center survey.

Though difficulty in executing a search warrant represents the most visible form of the computer search and seizure problem, it is hardly the only one. Since the nature of computers involves numerous opportunities for electronic access, and many possible intruders, it should not be too surprising that different investigative techniques may be necessary to detect computer criminals. However, different investigation methods may well trigger novel search and seizure arguments challenging the appropriateness of the innovation.

For example, in one case two employees of New York's Department of Motor Vehicles would collect registration payments, then issue orders to the DMV computer to cancel the transaction fees. Once the transaction was cancelled, they felt safe keeping the money. After the crime was discovered, considerable effort was required to reprogram the DMV system to, in effect, monitor the defendants and numerous other employees of the Department of Motor Vehicles. Ultimately, the surveillance led to the two individuals who pled guilty in this case. In Los Angeles and Tokyo, computers were similarly programmed to detect when they were being used without permission, as well as the location of illicit users.

These cases demonstrate some of the novel search-fact situations on which defense attorneys may meditate. To challenge searches as infringements of rights unanticipated by the founders of the Constitution is not without rewards.

History has shown that the far-out theory of one era becomes the dogma of the next. Already, in the case of United States v. Palmer and Kelley, a Pennsylvania case involving two employees of Univac who used part of the company's computer to attempt to run their own business, the legality of the surveillance of the defendants was raised as a major (but unsuccessful) aspect of the defense case.

CHARGING COMPUTER CRIMES

The most immediate and likely problem for an attorney reviewing a computer crime case is the applicability of the state or federal legislation defining computer crime. The proposed Federal Computer Systems Protection Act (S 240), has led to a considerable amount of attention to computer crime.

* * * *

Three cases where prosecution was difficult because no legislation specifically covered computer crimes were discussed by respondents to the NCCCD survey:

In U.S. v. Kelley and Palmer (U.S. District Court, Philadelphia, #77-250), the defendants set up a computerized sheet music arranging and engraving company using their employer's computer. They were charged with using the mails to defraud (18 USC 1341) because they sent out brochures which failed to state they were using their employer's computer and not their own.

In U.S. v Sampson and Miller (U.S. District Court, Northern California) the first case of theft of computer time was brought under 18 USC 641, which makes theft of government property a crime.

Finally, in U.S. v. Kostoff et al (U.S. District Court, Los Angeles), the prohibition against making false statements in loan applications (18 USC 1014) was used against a group which created false credit information for a fee.

To deal with the problems posed by cases such as the three just summarized, Ribicoff's S 240 would make it a federal crime to access, or in any way use, a computer for fraudulent purposes. These purposes include theft, sabotage, and embezzlement. The bill also gives four examples of what access means. These are: tampering with input data, using computer facilities for illegal purposes, altering or destroying data within a computer system, and stealing money, property, or

confidential information through the manipulation of computer output.

* * * *

PUBLICITY

From the time a computer crime case is filed, if not before that, it is far more likely to draw publicity than would a comparable noncomputer crime case. Obviously, a case such as the multi-million dollar theft of Security Pacific Bank by the bank's former consultant, Stanley Mark Rifkin, is not easily ignored. But even when the take is not overwhelming and the method not particularly novel, the newspapers are likely to pick up a case involving computer crime.

Newspapers, radio and television seem quite willing to play a role in the creation of a computer myth. This myth sees computer criminals as weird geniuses who in some way beat the system and thus deserve both criticism and acclaim. In the Security Pacific Bank case, Mark Rifkin penetrated a computer system to transfer $10.2 million of the bank's money to an account in Switzerland. Stories in the Los Angeles Times focused on the fact that bank officials were unaware of Rifkin's theft until the FBI reported it to them and on what the Times called the government's loss of "key evidence." However, this loss was not a crucial blow to the prosecution since a tape of the criminal act was not suppressed.

* * * *

. . . Computer myths mean that cases which otherwise would be left in relative obscurity will be publicized. And it means that many of these cases will be reported badly.

* * * *

Despite the problems resulting from greater media interest in computer crime cases, few successful techniques have been devised to cope with the effects of this publicity. NCCCD survey replies indicate few attempts to counteract it. Some motions for change of venue were considered and not filed, and some were filed without success. . . .

To date NCCCD has not seen documentation of any sophisticated publicity-limiting measures, such as gag orders or the like. Nonetheless, one can only assume that in the right case the same considerations which have been listed by other authors[7] would be applicable in the trial of a highly publicized computer crime case. . . .

* * * *

TRIAL

Computer crime cases are tried even less frequently than most criminal matters. Respondents to NCCCD's computer crime survey in several instances indicated surprise that more computer crime cases were not tried. (Most of those expressing surprise were prosecutors who apparently saw more potential weaknesses in their own cases, than the attorneys working on the defense side of the issues. However, in view of the generally light sentences which accompanied many guilty pleas, this defense strategy is perhaps understandable.) As a consequence of this apparent disinclination to go to trial, convincing the trier of fact and getting evidence admitted to trial are issues about which little can be said based on actual case experience. Those attorneys who actually tried computer crime cases did not experience great difficulty in communicating with the jury, according to their reports. Each stressed the need to spend a considerable time in self-education. To accomplish this goal, some read standard general-information books like Donn Parker's Crime By Computer, or Thomas Whiteside's Computer Capers. Some attended a course in computer crime, such as that given by Professor Edward Coughran of UC, San Diego. And just about all had lengthy discussions with experts who explained the nature of the crime and the nature of the underlying computer system to them.

None of the prosecutors involved in the survey experienced any difficulty in finding experts. Victim companies provided expertise when needed. Those defense attorneys who hired independent experts indicated no unusual difficulties in getting them, understanding them, or examining them. One general warning which was applied to the area of computer crime is the need to remember that computer experts are not necessarily accounting or security experts and that their testimony should be carefully focused within the realm of their expertise.

The admissibility of computerized evidence has been extensively discussed in cases and legal periodicals.[8] Again, surprisingly little of this discussion seems to have been relevant in any of those computer crime cases that were actually tried. The theoretical problems that face the proponent of the admission of computer-based evidence are staggering. To establish completely the reliability of a computer system that produces a document (or some other form of information) would entail establishing that the system was adequately secured against intentional abuse or negligent harm.[9] This is a task that few computer owners would relish undertaking. The problem noted by the expert in the Lyle case quoted above is true of most significant systems. To explain fully the reliability of a computer system to a judge would require a rather extensive and painstaking course in computer

programming, systems design, and many other subspecialities of the computer field. The enormity of the task may even work against the defense attorney seeking to put the prosecution to this burden of proof. George Monaco, chief of the Cook County District Attorney's Fraud Bureau, responded to a defense motion asking him to produce proof of a computer system's reliability, by saying, "Judge, if the court has no objection to clearing its calendar for the next year, I will be delighted to bring in the experts necessary to explain to the court everything it could possibly want to know about how this computer works." "Motion denied," the judge responded.

SENTENCING

In light of the sparsity of computer crime trials, the importance of the sentencing phase of a computer crime case cannot be overstated. Furthermore, a number of factors contribute to make this one of the most challenging aspects of the computer crime case. Although specific fact situations vary, of course, the typical computer crime case presents a sentencing judge with a very difficult decision. For the most part, he or she will be looking at an inexperienced defendant. In cases that have come to the attention of NCCCD, no defendant has had any serious prior contacts with the law. In most cases, the individual was white, middle class, gainfully employed, and well-regarded in the community. Where a loss was sustained, often the victim was a business that pursued the defendant or defendants civilly and got a judgment for the total loss or the defendant's promise of restitution. Often the defendant's actions were not far from common practice in the computer industry. In some of the cases surveyed, novel theories of law were used and the defendants were the first individuals ever convicted of computer crime under the statutes pled by the prosecutors.

* * * *

ENDNOTES

[1]General discussions are available: Bequai, Computer Crime (1978); Bequai, Legal Problems in Prosecuting Computer Crime, 21 Security Management 26 (1977); Coughran, Computer Abuse and Criminal Law (published by U.C. San Diego Computer Center) (1976); Coughran, Outlook For Prosecution In Computer Abuse Cases, 1 Criminal Justice Journal 397 (1978); Hemphill and Hemphill, Prosecuting Computer Criminals, 14 Security World 62 (1978); Holman, Computer Crime: A Prosecutor's Perspective, 1979 Honeywell Computer Security and Privacy Symposium Proceedings. Notably absent are any studies of the defense of a computer crime case.

[2]This article is an abridged version of a study to appear in the Computer Law Journal's Computer Crime issue (scheduled for publication in January 1980). The complete results of the survey should be available at that time, respondents willing.

[3]The National Center for Computer Crime Data is a clearinghouse for information about computer crime investigation and prosecution. The author, Jay Becker, is its director.

[4]Compare PEOPLE v. SUPERIOR CT. (Williams), 77 Cal App. 3d 69 (1978) with PEOPLE v. SUPERIOR CT. (Myers), 25 Cal 3d 67 (1979).

[5]Most notable of these noncomputer search and seizure issues was the one raised in the Rifkin case. See the discussion of this case below in the section dealing with publicity.

[6]Best, The Trial Lawyer's Role in the Sensational Case, in Advanced Criminal Trial Tactics, PLI Court Handbook No. 103, at 221-232 (1978); Ferber, Beating Bad Press: Protecting the California Criminal Defendant from Adverse Publicity, 10 U.S.F.L. Rev. 391 (1976); Hurson, The Trial of a Highly Publicized Case: A Prosecutor's View, 16 Am. Crim. L. Rev. 473 (1979); Younger, Some Thoughts on the Defense of Publicity Cases, 29 Stan. L. Rev. 591 (1977); Jones, Handling the High Publicity Case, in Advanced Criminal Trial Tactics, PLI Course Handbook No. 103, at 153-174 (1978); Isaac, The Psychology of Trying the Publicized Case, in Advanced Criminal Trial Tactics, PLI Course Handbook No. 103 at 175-184 (1978).

[7]Abelle, Evidentiary Problems Relevant to Checks and Computers, 5 J. Computers and Law 323 (1976); Bender, Computer Law: Evidence and Procedure (1978) (Chapters 5, 6); Freed, Computer Print-Outs as Evidence, 16 Proof of Facts 273; Goger, Proof of Public Records Kept or Stored on Electronic Computing Equipment, 71 ALR 3d 232; DeHetre, Data Processing Evidence: Is It Different?, 52 Chic.-Kent L. Rev. 567 (1976); Sprowl, Evaluating the Credibility of Computer-Generated Evidence, 52 Chic.-Kent L. Rev. 547 (1976); Note, A Reconsideration of the Admissibility of Computer-Generated Evidence, 126 U. Pa. L. Rev. 425 (1977); MONARCH FEDERAL SAVINGS AND LOAN ASSN v. GENSER, 383 A.2d 475 (1977); Tapper, Computer Law, Chapter 6 (1978).

[8]The best summary of these problems is found in Note, A Reconsideration of the Admissibility of Computer-Generated Evidence, 126 U. Pa. L. Rev. 425 (1977).

☆ U.S. GOVERNMENT PRINTING OFFICE : 1980 O—311-379 (1316)

END