COMPUTER CRIME

Criminal Justice Resource Manual

National Criminal Justice Information and Statistics Service
Law Enforcement Assistance Administration
U.S. Department of Justice

U. S. DEPARTMENT OF JUSTICE
Law Enforcement Assistance Administration

Henry S. Dogin, Administrator

Homer F. Broome, Jr., Deputy
Administrator for Administration

Benjamin H. Renshaw, Acting
Assistant Administrator
National Criminal Justice Information
and Statistics Service

Carol G. Kaplan
Director, Privacy and Security Staff

COMPUTER CRIME

Criminal Justice Resource Manual

National Criminal Justice Information and Statistics Service
Law Enforcement Assistance Administration
U.S. Department of Justice

This document was prepared for the National Criminal Justice Information and Statistics Service of the Law Enforcement Assistance Administration, U.S. Department of Justice, under Grant No. 78-SS-AX-0031 awarded to SRI International. Points of view and opinions stated herein are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice or of SRI International.

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

Stock Number 027-000-00870-4

EXECUTIVE SUMMARY AND GUIDE

Computer-related crime is defined for the purposes of this manual as any illegal act for which knowledge of computer technology is essential. Prosecutors are well advised to treat cases involving computers within the context familiar to them and the courts. They should minimize technical aspects that may confuse lay persons and thus lead to reasonable doubt acquittals. Therefore, the purpose of this manual is to provide prosecutors and investigators with both the simplest, most straightforward means of successfully prosecuting computer-related perpetrators and the technical context when needed.

The manual is written for prosecutors and investigators who know little about computer technology and those with extensive technical knowledge. For lay persons, this manual is an aid to determine when technical expertise should be used and how to interact with the people who provide it. The investigator or prosecutor experienced in computer technology will find much information that will assist in dealing with the most sophisticated of computer-related crimes.

To facilitate understanding in using the manual, it is recommended that the computer technology novice start first by studying Section VI, "Overview of Computer Technology," and using the glossary of terms in the front of the manual. The glossary also provides a quick reference for other readers encountering unfamiliar technical terms in the text. The glossary was derived from commonly used definitions and from legal definitions in computer-related crime laws and legislative bills. A cross-reference index at the back of the manual will assist readers in locating a specific subject.

The manual is written in a form combining legal, technical, and investigative concepts. The first four sections of the manual follow the typical order of events for prosecutors and investigators in handling a criminal case. The sections are Classifying the Crime; Experts, Witnesses, and Suspects; Discovering the Crime; and Making the Case. Each section starts with a description of the content of that section, how it may be used, and its relevance to investigators and prosecutors. Those searching for the law applicable to computer-related crime should read Section V on computer-related law. It was written by an attorney for attorneys and provides legal citations.

Appendixes A through C include copies of computer-related crime laws and proposed computer-related crime legislation as of the date of this writing. Some of this material will be out of date rapidly as legislation progresses. Therefore, the state legislature for any particular bill should be contacted to ensure that the most recent information is obtained. Appendixes D through G supply backup information for subjects referenced in text.

The summary of this manual presented below describes the contents of each section and the appendixes. This summary also serves as another aid for identifying and locating a specific subject for more detailed information.

SECTION I: CLASSIFYING THE CRIME

The nature, scope, definitions, classifications, and history of computer-related crime and experience with it are encapsuled in the first five subsections. The final subsection explains 12 technical methods used to perpetrate computer-related crime, including data diddling, Trojan horses, salami techniques, superzapping, logic bombs, data leakage, and piggybacking. Following the description of each technique is a table indicating potential perpetrators, methods of detection, and the kinds of evidence most likely associated with each. The skills, knowledge, and access of potential perpetrators in 17 occupations and likely vulnerabilities they may take advantage of are provided in Appendix D. The methods of detecting crimes and obtaining evidence are discussed in more detail in other sections of the manual.

Computer-related crime is the same in name as other familiar types of crime, including fraud, larceny, embezzlement, theft, sabotage, espionage, vandalism, burglary, extortion, and conspiracy. However, relative to the occupations of perpetrators, environments, modi operandi, forms of assets lost, time scales, and geography, many computer-related crimes differ significantly from traditional crimes. The nature of business, economic, and white-collar crimes is changing rapidly as computers pervade the activities and environments in which these crimes occur. Computers are therefore engendering a new kind of crime in which they play four roles as objects, subjects, instruments, and symbols for deception. Based on a study of 669 cases of computer-related crime over the past 20 years, the incidence of computer-related crime is increasing rapidly. This reflects the proliferation of computers in all segments of business; local, state, and federal government; and in society in general. At the same time, prosecution experience is increasing rapidly; hundreds of cases involving computers to varying degrees are currently being prosecuted.

SECTION II: EXPERTS, WITNESSES, AND SUSPECTS

Although considerable emphasis is focused on technical aspects, computer-related crime is basically a "people" problem. Therefore, to assist investigators and prosecutors with the people aspects of computer-related crime, this section describes the roles of computer technologists, with special emphasis on the computer security specialist and EDP (electronic data processing) auditor who can provide technical assistance.

Of equal importance to investigators and prosecutors are the various kinds of suspects in computer-related crime. Therefore, this section also deals with vulnerabilities of computer systems to crime

perpetrated by people in specific occupations. Characteristics of known computer criminals and aids for interviewing suspects are included.

The use of experts in the investigation and prosecution of computer-related crime, as in any other technical field, is particularly important. The best sources for obtaining experts are the victim's technical staff, the computer manufacturer of the equipment used, other organizations that use identical computer equipment and similar computer programs, local universities, computer technology consulting services, and service bureaus having similar equipment.

Distinctions are made among computer technologists who specialize in electronics, programming, and operations and also among data providers, users, systems analysts, and programmers who specialize in scientific/engineering information and business applications. Organizations are also discussed that use computers to conduct their business; manufacture computers, computer programs, and supplies; and provide computer services as a business.

SECTION III: DISCOVERING THE CRIME

The purpose of this section is to lead the investigator through the unique physical environments of computers, operational procedures, and vulnerabilities in the use of computers to provide the necessary insights and familiarity to be effective in discovering a computer-related crime. To this end, the first three subsections describe the operational, physical, and computer-usage environments the investigator is likely to encounter. The last subsection describes points in computer centers that are susceptible to criminal acts.

This section provides a relatively technical description of the functions in a computer center. The discussion of the operation of the equipment and of physical facilities particularly emphasizes the safeguards and controls that may be violated in the perpetration of a crime. Descriptions of 11 typical computer-generated, periodic reports about the operation of a computer are presented as a valuable source for discovering evidence of a crime. A description of computer usage in science/engineering and business applications provides a basis for the subsequent description of computer system functional vulnerabilities taken from actual experience and physical locations of vulnerabilities. This provides the investigator with the potential sources where criminals acts are most likely to occur. The section concludes with a discussion of the natural forces that can be used successfully to cause substantial damage to fragile computer systems. Various forces, such as magnetic fields, projectiles, heat, cold, moisture and chemicals, are identified.

SECTION IV: MAKING THE CASE

This section is designed to aid in the practical application of technical knowledge of computers to the case development and prosecution

of computer-related crime. Investigators and prosecutors are assumed to already be trained in investigative and prosecution techniques. Therefore, this section focuses only on those aspects of case development that require application of knowledge about technology, environments, job responsibilities, operations, and security provisions with regard to computers as described in previous sections.

Generally, before proffered physical evidence can be admitted into evidence, certain foundational 'preliminary facts' must be proved by the party seeking admission. These preliminary facts are to be contrasted with the facts sought to be proved by the evidence. Quite obviously a principal defense tactic will be to attack admissibility based upon foundational issues, an attack to which the prosecutor is particularly vulnerable. The prosecutor may have to match his experts with those of the defense. Therefore, the more knowledgeable and competent experts, who have been more directly involved in the evidence-producing processes and who are the more effective witnesses on the stand, will prevail. A team approach to the development of a technically complex case is recommended. A team comprising an investigator, a prosecutor, a computer expert, and an EDP auditor would be ideal.

Therefore, the discussion in this section concentrates on computer-related evidence. A detailed step-by-step method of producing computer-generated reports is presented to ensure that the integrity of the production methods and the contents of the reports will not be easily challenged. Caring for evidence in the form of magnetic tapes and disks is also discussed. There is a subsection on legal definitions in computer technology and another on propriety rights of computer programs, evidentiary problems with computer records, admissibility of computer printouts as evidence, and computer records as the basis for expert testimony.

Practical recommendations for prosecutors conclude this section. The discussion covers such factors as expert witnesses' testimony, technical presentations, immunity, and judges' understanding of the technology. Technical presentations in a court can sometimes be aided by using analogies: phonograph records for magnetic disks, typewriters for computer terminals, food recipes and player piano rolls for computer programs, and combination locks for terminal access passwords. Computer field jargon such as software, firmware, bits and bugs should be avoided because of ambiguity of these terms. Visual aids, such as pocket calculators to illustrate input, output, storage and number representation and installation of a computer terminal in the courtroom also can be used to demonstrate time-sharing concepts.

One of the traps a prosecutor may face is the challenge to his claim that a computer was involved in an alleged crime and that a computer crime law is applicable. Basic advice is to minimize the computer's role and to prosecute on the basis of the criminal law most familiar to the prosecutor and the court. For example: taking a computer program may be prosecuted as a simple property theft. On the

other hand, it may be reasonable to make the case for a program theft by presenting definitions of what constitutes a computer program and what constitutes taking it from a computer storage device in object form or in uncompiled form in source code. A more detailed knowledge of computer technology is required to understand the applications in this section than in the other sections; therefore, it is advisable to first have a good grasp of the contents of Section VI.

SECTION V: COMPUTER-RELATED CRIME LAW

The purpose of this section is to aid prosecutors by identifying and summarizing existing state and federal statutes and proposed legislation applicable to computer-related crime. Prosecutors have stated that statutes have been found that are applicable to the prosecution of all cases of computer-related crime coming to their attention. However, the laws were not written in anticipation of high-technology crime, and in some cases prosecution has been difficult and obtuse.

The need for laws directly applicable to computer-related crime has recently been recognized, and they are currently under development. Hence, new laws are being adopted at such a rapid rate that a completely timely discussion of computer crime law is difficult. Accordingly, this section is expected to be partially obsolete by the time it is published, and updates of this section will be needed soon thereafter. The urgent need for a summary of applicable law, however, justifies the writing.

Appendixes A, B, and C supplement this section by providing copies of computer-related crime, federal and state statutes, and current legislative bills. Appendix G is a reference to legal action in selected cases providing brief descriptions of 133 cases reported since 1972. The list is not represented as being complete, either as to numbers of cases or to disposition of any given case. Instead, the intent is that the references will provide a starting point for prosecutors who have similar fact patterns.

SECTION VI: OVERVIEW OF COMPUTER TECHNOLOGY

Prosecutors and investigators probably will seldom encounter cases requiring the detailed information presented in this section. If they do have such cases, expert assistance should usually be obtained. The information presented in this section not only will aid in dealing with these experts, but also will prepare prosecutors for the possibility of the defense introducing technical concepts in a trial.

This section describes what makes a computer work, the data structure, and the coding of input data to a computer. It also provides explanations of computer programming techniques; programming languages; computer systems structure; data communications and teleprocessing; and the concepts of batch, real-time, on-line, and time-sharing modes of

using computers. This section also uses many diagrams and photographs to aid in further understanding of the technology. Appendix F provides examples of computer terminal printouts from sessions using three national time-sharing services. Detailed descriptions of the contents of the printouts provides a basic understanding of on-line interaction with a computer.

CONCLUSION

This manual is the first comprehensive document designed specifically to aid investigators and prosecutors in dealing with computer-related crime. The subject is nearly as complex and comprehensive as forensic medicine and is also expected to be an equally common subject in the criminal justice community. Capabilities and specialized experts within the criminal justice community will evolve as computer technology becomes a significant focus for business-related and white-collar crime. Much new literature will follow the publication of this first definitive manual on the subject. In the meantime, it is anticipated that it will be a useful document readily available to all prosecutors and investigators in the criminal justice community.

CONTENTS

CONTENTS (Continued)

ILLUSTRATIONS

TABLES

TABLES (Concluded)

GLOSSARY OF TECHNICAL TERMS

This glossary provides, in layman's terms, the contemporary meanings of the specialized data processing terms used in this manual. The glossary may be used as an independent source of information to clarify terms the prosecutor encounters both in investigation and in court. Where useful, definitions have been extracted from other recognized glossaries and computer crime legislation. The prosecutor can readily note that a definition is from a computer crime law or bill because it is enclosed in quotation marks. The numbers following some definitions refer to the source, as is listed below.

The entries are arranged in alphabetical order; special characters and spaces between words are ignored. Acronyms are placed in the same sequence as other terms, according to their spelling. When two or more terms have the same meaning, definitions are given only under the preferred term. Other relationships between terms are set forth at the end of the definition, as are cross references. Upper case terms in definitions refer to terms also defined in the glossary.

GLOSSARY CITATIONS

[1] Florida Computer Crimes Act (See Appendix B).

[2] Colorado Computer Crime Act (See Appendix B).

[3] Arizona Criminal Code, 13-2301 (See Appendix B).

[4] Proposed California Senate Bill No. 66 Introduced by Senator Cusanovich; December 5, 1978 (See Appendix C).

APPLICATION PROGRAM: A COMPUTER PROGRAM, written for or by a computer user, that causes a COMPUTER SYSTEM to satisfy his purposes.

APPLICATIONS PROGRAMMER: One who designs, develops, DEBUGS, installs, maintains, and documents APPLICATION PROGRAMS.

ASSEMBLER: A COMPUTER PROGRAM that translates COMPUTER PROGRAM instructions written in ASSEMBLY LANGUAGE into MACHINE LANGUAGE.

ASSEMBLY LANGUAGE: A SOURCE LANGUAGE that includes symbolic MACHINE LANGUAGE statements in which there is a one-to-one correspondence with the instructions in the form of MACHINE LANGUAGE of the computer.

ASYNCHRONOUS ATTACKS: Taking advantage of the asynchronous nature of computer OPERATING SYSTEMS to perpetrate an unauthorized act, e.g., confusing the queuing of jobs awaiting servicing.

AUDIT TRAIL: A sequential record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of states and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

BASIC (Beginners All-Purpose Symbolic Instruction Code): An algebra-like computer programming language used for problem-solving by engineers, scientists, and others who may not be professional PROGRAMMERS. Designers of the language intended that it should be a simplified derivative of FORTRAN.

BATCH PROCESSING: The processing of DATA or the accomplishment of jobs accumulated in advance in such a manner that each accumulation thus formed is processed or accomplished in the same computer run.

BIT (BInary digiT):

(1) In the binary numeration system, either of the digits 0 or 1.

(2) An element of DATA that takes either of two states or values.

BYTE: A sequence of usually 6 or 8 BITS operated upon as a unit and often part of a computer WORD. This sequence may represent a character.

CHECKPOINT RESTART: A point in time or processing sequence in a machine run at which processing is momentarily halted to make a record of the condition of all the variables of the machine run, such as the position of input and output (I/O) tapes and a copy of the contents of working storage. This process, in conjunction with a restart routine, minimizes reprocessing time occasioned by machine or other failures.

COBOL (COmmon Business-Oriented Language): A HIGH-LEVEL computer programming language designed for business data processing.

COM (Computer Output Microfilm):

(1) Microfilm that contains DATA that are received directly from computer-generated signals.

(2) To place computer-generated DATA on microfilm.

(3) A recording device that produces computer output microfilm.

COMMUNICATIONS ENGINEER/OPERATOR: One who operates communications equipment including concentrators, multiplexors, modems, and line switching units. Ordinarily, this person reconfigures the communications network when failures or overload situations occur.

COMPILER: A COMPUTER PROGRAM used to translate a COMPUTER PROGRAM expressed in a problem-oriented language (SOURCE CODE) into MACHINE LANGUAGE (OBJECT CODE).

COMPUTATION BOUND: The state of execution of a COMPUTER PROGRAM in which the computer time for execution is determined by computation activity rather than I/O activity.

Contrast with: I/O BOUND

COMPUTER:

(1) "...an internally programmed, automatic device that performs data processing." [1]

(2) "...an electronic device which performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network." [2]

(3) "...an electronic device which performs logic, arithmetic or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, software or communication facilities which are connected or related to such a device in a system or network." [3]

COMPUTER ABUSE: Any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator by intention made or could have made gain.

COMPUTER CRIME (See COMPUTER-RELATED CRIME)

COMPUTER NETWORK:

(1) "...a set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities. [1]

(2) "...the interconnection of communications lines (including microwave or other means of electronic communication) with a computer through remote terminals, or a complex consisting of two or more interconnected computers." [2]

(3) "...an interconnection of two or more computer systems." [4]

COMPUTER OPERATOR: A person who operates a computer, including duties of monitoring system activities, coordination of tasks, and the operation of equipment.

COMPUTER PROGRAM:

(1) "...an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data." [1]

(2) "...a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer in a manner designed to provide appropriate products from such computer system." [2]

(3) "...an ordered set of instructions or statements, and related data, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions." [4]

COMPUTER-RELATED CRIME: Any illegal act for which knowledge of computer technology is essential for successful prosecution.

COMPUTER SECURITY SPECIALIST: A person who evaluates, plans, implements, operates, and maintains physical, operational, procedural, personnel, and technical safeguards and controls that are related to the use of COMPUTER SYSTEMS.

COMPUTER SYSTEM:

(1) "...a set of related, connected or unconnected computer equipment, devices, or computer software." [1]

(2) "...a machine or collection of machines, used for governmental, educational, or commercial purposes, one or more of which contain computer programs and data, that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control." [4]

CPU (Central Processing Unit): The device in a COMPUTER SYSTEM that includes the circuits controlling the interpretation and execution of instructions. The term may also refer to the portion of the computer that contains its control, logic, and sometimes internal storage.

CRT (Cathode Ray Tube): A device that presents DATA or graphics in visual form by means of controlled electron beams. This electronic vacuum tube is much like a television picture tube.

DATA:

(1) DATA are a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or automatic means. DATA may be representations, such as characters or analog quantities, to which meaning is, or might be, assigned.

(2) DATA may be defined as any representation of fact or idea in a form that is capable of being communicated or manipulated by some process.

(3) "...a representation of information, knowledge, facts, concepts, or instructions, which are being prepared or have been prepared, in a formalized manner, and are intended for use in a computer system or computer network." [4]

Contrast with: INFORMATION

DATA BASE: An organized collection of DATA processed and stored in a COMPUTER SYSTEM.

DATA BASE ADMINISTRATOR: An individual with an overview of one or more DATA BASES, who controls the design and use of these DATA BASES. Responsiblities are the addition, modification, and deletion of records and frequently the security of the DATA BASE.

DATA COMMUNICATIONS: The transmission, reception, and validation of DATA.

DATA DIDDLING: The unauthorized changing of DATA before or during their input to a COMPUTER SYSTEM. Examples are forging or counterfeiting documents and exchanging valid computer tapes or cards for prepared replacements.

DATA ENTRY AND UPDATE CLERK: A person who adds, changes, and deletes records in computer-stored DATA BASES by means of a computer terminal, or manually updates punch cards or entries on input data forms for computer input.

DATA LEAKAGE: Unauthorized, covert removal or obtaining copies of DATA from a COMPUTER SYSTEM, e.g., sensitive DATA may be hidden in otherwise innocuous looking reports. This is a deliberate act whereas DATA seepage, the provision of DATA or information to unauthorized individuals, is accidental.

DATA SET (See FILE)

DBMS (Data Base Management System): A computer APPLICATION PROGRAM or set of programs that provides STORAGE, retrieval, updating, management, and maintenance of one or more DATA BASES.

DDA (Deputy District Attorney): An assistant to a District Attorney.

DEBUG: To detect, locate, and remove mistakes or malfunctions from a COMPUTER PROGRAM or COMPUTER SYSTEM.

DIRECT ACCESS: A method for the retrieval or storage of DATA, by reference to their addressable location in a STORAGE device, rather than to their location by position in a sequence.

Contrast with: SEQUENTIAL ACCESS

DISTRIBUTED PROCESSING: Electronic data processing (EDP) performed in computers near or at the sources of data and/or near the users of results where the data processing might otherwise be performed at a single, central site removed from data sources or users.

EDP (Electronic Data Processing) AUDITOR: A person who performs operational, computer, COMPUTER PROGRAM, and data file reviews to determine integrity, adequacy, performance, security, and compliance with organization and generally accepted policies, procedures, and standards. This person also may participate in design specification of applications to ensure adequacy of controls; performs data processing services for auditors.

EFTS (Electronic Funds Transfer System): A computer and TELECOMMUNICATION network to execute a wide range of monetary transfers.

FACILITIES ENGINEER: A person who inspects, adjusts, repairs, modifies, or replaces equipment supporting computer and terminal facilities, e.g., air conditioning, light, heat, power, and water.

FILE A collection of related DATA records treated as a unit. For example, one line of an invoice may form an item, a complete invoice may form a record, the complete set of records may form a FILE.

Synonym: DATA SET

FIRMWARE (computer jargon, not recommended for use): A COMPUTER PROGRAM that is considered to be a part of a computer and not modifiable by computer OPERATING SYSTEM or APPLICATION PROGRAMS. It often makes use of computer instructions not available for normal programming. It is often called a microprogram. The name is derived from other jargon terms, SOFTWARE and HARDWARE.

FORTRAN (FORmula TRANslation): A higher level programming language primarily used to write COMPUTER PROGRAMS that tend to be more engineering- or scientific-oriented rather than business-oriented.

FRONT-END PROCESSOR: A special-purpose computer used to reduce the work load of the main computer primarily for input, output, and data communications functions.

HARDWARE (computer jargon, not recommended for use): The computer and all related or attached machinery, such as mechanical, magnetic, electrical, and electronic devices, used in data processing.

Contrast with: SOFTWARE

HIGH-LEVEL LANGUAGE: A programming language that is independent of the structure of any one given computer or that of any given class of computers. Some particular languages are designed for specialized applications.

Contrast with: ASSEMBLY LANGUAGE

INFORMATION: The meaning that a human assigns to DATA by means of conventions used in their representation.

See: DATA

INSTRUCTION: A statement appearing in a COMPUTER PROGRAM that specifies an operation and the values or locations of its operands.

INSTRUCTION LOCATION: The place or address where DATA in the form of an INSTRUCTION, may be stored within a COMPUTER SYSTEM.

INTERACTIVE: The mode of use of a COMPUTER SYSTEM in which each action external to the COMPUTER SYSTEM elicits a timely response. An interactive system may also be conversational, implying a continuous dialog between the user and the COMPUTER SYSTEM.

I/O BOUND: The state of execution of a COMPUTER PROGRAM in which the computer time for execution is determined by I/O activity rather than computation activity.

Contrast with: COMPUTATION BOUND

JCL (see JOB CONTROL LANGUAGE)

JOB: A set of DATA and COMPUTER PROGRAMS that completely define a unit of work for a computer. A job usually includes all necessary COMPUTER PROGRAMS, mechanisms for linking COMPUTER PROGRAMS, DATA, FILES, and INSTRUCTIONS to the OPERATING SYSTEM.

JOB CONTROL LANGUAGE: A programming language used to code job control statements. A job control program is a COMPUTER PROGRAM that is used by the COMPUTER SYSTEM to prepare each job or job step to be run.

JOB QUEUE: A sequenced set of JOBS in COMPUTER STORAGE arranged in order of assigned priority for execution by a computer.

JOB SETUP CLERK: A person who assembles jobs. This task includes compilation of DATA, COMPUTER PROGRAMS, and job control information. This person requests that JOBS be executed, requests media libraries for necessary DATA, physically places jobs and DATA into JOB QUEUES, handles procedures for reruns, and possibly distributes output to users.

LOAD AND GO: A computer operation method by which higher level language programs or JOBS are entered, prepared for execution, and immediately executed.

LOCAL PROCESSING: Data processing that is conducted near or at the user's location, rather than at a remote CPU.

LOGIC BOMBS: A COMPUTER PROGRAM residing in a computer that is executed at appropriate or periodic times to determine conditions or states of a COMPUTER SYSTEM and that facilitates the perpetration of an unauthorized act.

LOOP: A sequence of INSTRUCTIONS in a COMPUTER PROGRAM that is executed repeatedly until a terminal condition prevails.

MACHINE LANGUAGE: A computer programming language that is used directly by a computer, without having to pass through a translation program, such as a COMPILER.

MAIN STORAGE: The fastest access STORAGE device in a COMPUTER SYSTEM where the storage locations can be addressed by a COMPUTER PROGRAM, and INSTRUCTIONS and DATA can be moved from and into registers in the CPU from which the INSTRUCTIONS can be executed or from which the DATA can be operated upon.

MASTER FILE: A FILE of DATA that is used as an authority in a given JOB and that is relatively permanent, even though its contents may change from run to run.

MEDIA LIBRARIAN: A person who files, retrieves, and accounts for OFF-LINE storage of DATA on disk, tape, cards, or other removable data STORAGE media. The person provides media for the production control and job set-up areas and functions, and cycles backup files through remote STORAGE facilities.

MEDIUM: The material, or configuration thereof, on which DATA are recorded. Examples are punched paper tape, punch cards, magnetic tape, and disks.

MEMO UPDATE: A FILE update procedure whereby MASTER FILES are not directly modified to reflect each transaction. Instead, pointers to other files are used to keep track of updates to specified records. Pointers are used periodically to obtain the data to merge with and update a MASTER FILE.

MEMORY (See MAIN STORAGE)

MICR (Magnetic Ink Character Recognition): A standard machine-readable type font printed with magnetic ink on documents such as bank checks and deposit slips that can be directly read by machine.

MIS (Management Information System): An integrated man/machine COMPUTER SYSTEM for providing INFORMATION to support the operations, management, and decision-making functions in an organization. Ordinarily, the system utilizes management and decision models, and a DATA BASE.

MODEM (MOdulator-DEModulator): A device that modulates and demodulates signals transmitted over DATA TELECOMMUNICATION facilities. This transformation, i.e., conversion of digital signals to analog signals and back again, is necessary for use of common voice-grade telephone lines for COMPUTER communication purposes.

MULTIPROCESSING: The use of two or more CPUs in a COMPUTER SYSTEM under integrated control.

MULTIPROGRAMMING: The concurrent execution of two or more PROGRAMS accomplished by sharing the resources of a computer.

NETWORK (See COMPUTER NETWORK)

OBJECT CODE: Output from a COMPILER or ASSEMBLER that is executable MACHINE LANGUAGE.

Contrast with: SOURCE CODE

OCR (Optical Character Recognition): The machine identification of printed characters through use of light sensitive devices.

Contrast with: MICR

ON-LINE: The state of devices or computer users in direct communication with a CPU. Also a COMPUTER SYSTEM in an INTERACTIVE or TIME-SHARING mode with people or other processes.

Contrast: OFF-LINE

OPERATING SYSTEM: An integrated collection of COMPUTER PROGRAMS resident in a computer that supervise and administer the use of computer resources to execute jobs automatically.

OPERATIONS MANAGER: The manager of a computer facility responsible for the operation of the COMPUTER SYSTEM. He may also be responsible for the maintenance, specification, acquisition, modification, and replacement of COMPUTER SYSTEMS or COMPUTER PROGRAMS.

OPERATOR (See COMPUTER OPERATOR)

PERIPHERAL EQUIPMENT OPERATOR: A person who operates devices peripheral to the COMPUTER that performs DATA I/O functions.

PIGGYBACKING: A method of gaining unauthorized physical access to guarded areas when control is accomplished by electronically or mechanically locked doors. For example, a person may follow another through the doors although he does not possess the required authorization to pass. Electronic piggybacking occurs when a computer or terminal covertly shares the same communication line as an authorized user. The host computer, to which they both transmit, is unable to distinguish between those signals of the authorized and those of the unauthorized user.

PIN (Personal Identification Number): A password that must be entered by a COMPUTER SYSTEM user to gain access to a specific APPLICATIONS PROGRAM. Most often the term is associated with retail computer banking devices such as Automated Teller Machines (ATMs).

PL/1: A High-Level computer programming language designed for use in a wide range of business and scientific computer applications.

POS (POINT-OF-SALE) TERMINALS: Computer terminals used for transaction recording, credit authorization, and funds transfer and typically are situated within merchant establishments at the point of retail sales.

PRODUCTION PROGRAM: A PROGRAM which has been DEBUGGED and tested and is considered no longer in the development stage. Such a PROGRAM is often part of a library of programs used for data processing.

PROGRAM (See COMPUTER PROGRAM)

PROGRAMMER: A person who engages in designing, writing, and testing computer PROGRAMS.

PROGRAMMING MANAGER: A person who manages computer PROGRAMMERS to design, develop, and maintain computer programs.

REAL-TIME: The actual time during which a physical process transpires. Also a computer operation mode in which a computation takes place during the actual time that the related physical process transpires in order that results of the computation can be used in controlling and monitoring the physical process.

REMOTE JOB ENTRY (RJE): Submission of jobs through an input unit that has access to a computer through a DATA COMMUNICATIONS link.

REMOTE PROCESSING: Data entry and partial or complete processing near the point of origin of a transaction. Remote processing systems typically edit and prepare DATA input before transmission to a central computer.

ROM (Read-Only Memory): A semiconductor storage device in which the data content is fixed, readout is nondestructive, and DATA are retained indefinitely even when the power is shut off. In contrast, RAMs (Random-Access read/write Memories) are capable of read and write operations, have non-destructive readout, but stored DATA is lost when the power is shut off.

RPG (Report Program Generator): A High-Level computer programming language that is report-rather than procedure-oriented. PROGRAMMERS describe the functions desired of the computer by describing the output report.

RUN BOOK: A document containing INSTRUCTIONS for COMPUTER OPERATORS detailing operations set up procedures, job schedule checklists, action commands, error correction and recovery instructions, I/O dispositions, and system backup procedures.

SALAMI TECHNIQUES: The unauthorized, covert process of taking small amounts (slices) of money from many sources in and with the aid of a computer. An example is the round down fraud, whereby remainders from the computation of interest are moved to a favored account instead of being systematically distributed among accounts.

SCAVENGING: A covert, unauthorized method of obtaining information that may be left in or around a computer system after the execution of a JOB. Included here is physical search (trash barrels, carbon copies, etc.) and search for residual DATA within the computer STORAGE areas, temporary storage tapes, and the like).

SECURITY OFFICER: A person who evaluates, plans, implements, operates, and maintains physical, operational, procedural, personnel, and technical safeguards and controls.

SEQUENTIAL ACCESS: An access method for storing or retrieving DATA according to their sequential order in a STORAGE device.

Contrast with: DIRECT ACCESS

SIMULATION AND MODELING IN A CRIME: The use of a computer as a tool for planning or controlling a crime. An instance of this would be the simulation of an existing process to determine the possibility of success of a premeditated crime.

SOFTWARE (Jargon, not recommended for use): "Computer Software means a set of computer programs, procedures, and associated documentation concerning the operation of a computer system." [1]

Contrast with: COMPUTER PROGRAMS, OPERATING SYSTEM

SOURCE CODE: INSTRUCTIONS in a computer programming language that are used as input for a COMPILER, interpreter, or ASSEMBLER.

Contrast with: OBJECT CODE

SPOOLING: The reading and writing of DATA for I/O on auxiliary STORAGE devices, concurrently with execution of other jobs, in a format for later processing or output operations.

STORAGE:

(1) The action of placing DATA into a STORAGE device and retaining them for subsequent use.

(2) A device used for retaining DATA or COMPUTER PROGRAMS in machine-readable and retrievable form.

STORAGE CAPACITY: The number of BITS, characters, BYTES, WORDS, or other units of DATA that a particular STORAGE device can contain.

SUPERZAPPING: The unauthorized use of utility COMPUTER PROGRAMS that violate computer access controls to modify, destroy or expose DATA in a computer. The name derives from an IBM utility program called "Superzap."

SYSTEM (See COMPUTER SYSTEM)

SYSTEM ENGINEER: A person who designs, configures, tests, diagnoses, assembles and disassembles, and repairs or replaces COMPUTER SYSTEM devices and components.

SYSTEMS PROGRAMMER: A person who designs, develops, installs, modifies, documents, and maintains OPERATING SYSTEM and utility programs.

TELEPROCESSING: The processing of DATA that are received from or sent to remote locations by way of telecommunication circuits.

TELEPROCESSING MONITOR: A computer OPERATING SYSTEM program that controls the transfer of DATA between the communication circuits and a computer and often does the user polling (turn-taking among users) as well.

TERMINAL ENGINEER: A person who tests, diagnoses, assembles and disassembles, repairs, and replaces terminals or their components.

TIME-SHARING: A method of using a computing system that allows a number of users to execute programs concurrently and to interact with the programs during execution. A time-shared computer is used by several users at once.

Related term: BATCH PROCESSING

TRANSACTION OPERATOR: A person who operates a computer transaction terminal by entering transactions for processing by a COMPUTER SYSTEM. An example of such a device would be a POS TERMINAL.

TRANSACTION SYSTEM: A COMPUTER SYSTEM that is used for processing transactions in a prescribed manner controlled by APPLICATION PROGRAMS.

TRAP DOOR: A function, capability, or error in a COMPUTER PROGRAM that facilitates compromise or unauthorized acts in a COMPUTER SYSTEM.

TROJAN HORSE: Computer INSTRUCTIONS secretly inserted in a COMPUTER PROGRAM so that when it is executed in a computer unauthorized acts are performed.

UPDATE-IN-PLACE: A method for the modification of a MASTER FILE with current DATA each time a transaction is received in a COMPUTER SYSTEM.

Contrast with: MEMO UPDATE

UTILITY PROGRAM: A COMPUTER PROGRAM designed to perform a commonly used function, such as moving DATA from one STORAGE device to another.

WIRETAPPING: Interception of DATA COMMUNICATIONS signals with the intent to gain access to DATA transmitted over communications circuits.

WORD: A sequence of adjacent characters or BITS considered as an entity in a COMPUTER.

FOREWORD

Like most prosecutors, I was wholly unprepared on the fatal morning when my boss told me to write a search warrant for the recovery of a computer program that a citizen was complaining had been stolen. The following hours convinced me that I had much to learn, and but for luck we may well have had to leave unredressed a theft that was later valued at $0.5 million. Computer use has expanded in the 7 years since People v. Ward, and the reported thefts have increased even more. The prosecutor who believes that even intricate crimes must be brought to ground no longer has a choice: Computers are part of all our lives, and the information they carry is as important to the lives and plans of the people we serve as is clean water and safe streets.

There is no question that the beeping little boxes are not our usual fare. A good fingerprint, prymark, or powder trace is much easier to deal with (and sometimes show up in these computer-related crimes, too). But they are part of the world in which we enlisted, and we have no more ethical justification to dodge them than our predecessors had to avoid horseless carriage crime. Moreover, you will discover that you can handle a computer-related crime without a masters in math, even as an engineering degree is no prerequisite to nailing an auto theft, nor a pathology minor to dispatching a murderer. Computers are not that difficult. Indeed, as Section IV herein makes clear, the biggest hurdle to prosecution is being ensnared by the jargon: the electronic red herring gambit is easly thwarted with a little confidence.

And that, in my opinion, is the great value of this manual. A novel it is not; but approached as a basic text, it will reward your reading and enhance your skills against that certain day when the case of computer-related crime is laid on your front counter.

Donald G. Ingraham
Senior Trial Deputy
District Attorney
Alameda County
California

ACKNOWLEDGMENTS

The effective control of computer-related crime is an interdisciplinary matter involving computer technology, law, crime investigation, and crime prosecution. It also requires forward-thinking administrators of research funding agencies to recognize the needs in this new area of crime. The project established to produce this manual was singularly endowed with the right human resources across these disciplines and administrators.

The project grew out of initial contact with Mr. Harry Bratt, then assistant administrator of the National Criminal Justice Information and Statistics Service (NCJISS) of the Law Enforcement Assistance Administration (LEAA), U.S. Department of Justice. The motivation for the project came from the 1976 and 1977 staff studies performed in the U.S. Senate Committee on Government Operations at the instigation of Senator Abraham Ribicoff, chairman of that committee. In addition, early ideas and encouragement were received in 1976 from Mr. Mark Richard, then acting chief of the Criminal Division, U.S. Department of Justice. Encouragement was also received from Mr. Nathaniel E. Kossack, then Director of the National Economic Crime Project of the National District Attorneys Association and currently council to the firm of Perito, Duerk and Carlson, P.C. These people continue to encourage and advise the project in meeting the challenge of computer-related crime. Another early contributor to approaches to study the problem is Franklin E. Alan, then a courts specialist with LEAA in Seattle, Washington.

Carol G. Kaplan, Director of the LEAA NCJISS Privacy and Security staff and Jack Katz, a member of the staff have served as grant monitors for the project. Their patience, guidance and advice have been instrumental in the success of the project and its final products.

Donald Ingraham, Senior Trial Deputy District Attorney, Alameda County District Attorney's Office, and Laurence Donoghue, Deputy District Attorney, County of Los Angeles, served as consultants in the analysis of field work and reviews of delivered products. Mr. Ingraham wrote the foreward to this manual, and Mr. Donoghue contributed to a section on evidence. Thanks are extended to the National District Attorneys Association and to Patrick Healy, Executive Director, and Arthur Del Negro, Jr., Director of the Economic Crime Project; and Nathaniel E. Kossack, consultant to the project, for their advice in field site selections and for conducting a mailed survey of their Economic Crime Project members. In addition, thanks are extended to District Attorneys Edward Rendell of Philadelphia, Robert M. Morganthau of New York City, and John K. Van De Kamp of Los Angeles County, and to their assistants, Michael M. Mustokoff, Roger Hayes, and Philip Wynn and the many deputies and investigators who provided their facilities and time for the field work. Cooperation of the Auerbach Corporation and Boeing Computer Services for use of written materials is gratefully acknowledged.

Within the Survey and Analysis of Computer Crime project, a multidisciplinary team has worked well to contribute to success. The field survey was led by Theodore Lyman and conducted with the assistance of Barbara DeCaro and Eleanor Myers of the SRI International Urban and Social Systems Division. The legal analysis and writing of part of Section IV and all of Section V was performed by Susan H. Nycum, partner of Chickering and Gregory law firm in San Francisco. Assistance in analysis and compiling material came from Richard Gottlieb, Katherine Mize, and Charles Wood in SRI's Information Systems Management Department. Researching and writing the computer technology sections of the manual were done by Timothy Roche and Roy Price, senior consultants in the same department. In addition, special thanks are given to Eileen Stevens, senior editor; Patricia Sanders, word processing system operator; and Louise Burnett and Sarah Ward, secretary typists.

Donn B. Parker
Project Director

SECTION I CLASSIFYING THE CRIME

This manual for investigation of computer-related crime and for prosecution of the perpetrator addresses a new kind of crime. The purpose of this manual is to prepare the investigator, prosecutor, judge, auditor, computer security specialist, and potential victims to deal with the new technology of computing and its attendant ramifications wherever they are associated with intentionally caused losses. This was a consideration in the preparation of the manual in this first effort funded by the U.S. Department of Justice, Law Enforcement Assistance Administration (LEAA).

Experience and legislative interest have shown that basing the treatment of computer-related crime on computer technology is of value for the criminal justice and business communities. Many computer-related crimes can be prosecuted successfully without delving deeply into the technology. Many more of them, however, are sufficiently different from traditional crimes relative to the occupations of perpetrators, environments, modi operandi, forms of assets lost, time scales, and geography to identify the subject as a unique type of crime that warrants explicit capabilities and action.

A. THE NATURE OF COMPUTER-RELATED CRIME

Business, economic, and white-collar crimes are changing rapidly as computers proliferate into the activities and environments in which these crimes occur. Computers are engendering a new kind of crime.

The introduction of new occupations has extended the traditional categories of criminals to include computer programmers, computer operators, tape librarians, and electronic engineers who function in environments that are new. Whereas crime has traditionally occurred in environments of manual human activities, some crime is now perpetrated inside computers in the specialized environment of rooms with raised flooring, lowered ceilings, large grey boxes, flashing lights, moving tapes, and the hum of air-conditioning motors.

The methods of committing the crime are new. A new jargon has developed, identifying automated criminal methods such as data diddling, Trojan horses, logic bombs, salami techniques, superzapping, piggybacking, scavenging, data leakage, and asynchronous attacks (see Section I.F). The forms of many of the targets of computer-related crime are also new. Electronic money as well as paper money and plastic money (credit cards) now represent assets subject to intentionally caused loss. Money in the form of electronic signals and magnetic patterns is stored and processed in computers and transmitted over telephone lines. Money is debited and credited to accounts inside computers. In fact, the computer is rapidly becoming the vault for the business community. Many other physical assets, including inventories

of products in warehouses and of materials leaving or entering factories, are represented by documents of record inside computer systems.

The timing of some crimes is also different. Traditionally, the time of criminal acts is measured in minutes, hours, days, weeks, months and years. Today some crimes are being perpetrated in less than 0.03 of a second (3 milliseconds). Thus, automated crime must be considered in terms of a new time scale because of the speed of the execution of instructions in computers.

Geographic constraints do not inhibit perpetration of this new crime. A telephone with a computer terminal attached to it in one part of the world could be used to engage in a crime in an on-line computer system in any other part of the world.

All these factors must be considered in dealing with the new crime of computer abuse. Unfortunately, however, the business community, constituting all businesses, government agencies, and institutions that use computers for technical and business purposes, is neither adequately prepared to deal with nor sufficiently motivated to report this new kind of crime to the authorities. Although reliable statistics are as yet unavailable to prove this, computer security studies for the business community and interviews with certified public accountants have indicated that few crimes of this type are ever reported to law enforcement agencies for prosecution. On the one hand, many businessmen complain that even when they do report this crime, prosecutors frequently refuse to accept the cases for a variety of reasons, including their lack of understanding of the technology and their already heavy case loads. On the other hand, prosecutors and investigators indicate that the victim's records and documentation of crimes associated with computers in the business community are inadequate for effective prosecution.

B. DEFINITION OF COMPUTER-RELATED CRIME

Computers have been involved in most types of crime, including fraud, theft, larceny, embezzlement, bribery, burglary, sabotage, espionage, conspiracy, extortion, and kidnapping. Criminal justice agencies having limited experience with computer-related crime have generally thought of it as crime that occurs inside computers. This narrow definition has recently broadened as the proliferation of computers into most societal functions proceeds at an increasing pace. The public media have added to the confusion through sensationalized, distorted, often incorrect reporting by journalists and their sources who do not sufficiently understand the technology.

Computer-related crime is not well understood in the criminal justice and business communities, and no consensus on its definition exists. One definition is that it is a form of white-collar crime committed inside a computer system; another definition is that it is the use of a computer as the instrument of a business crime. An application of the former definition is making unauthorized changes to a computer program to transfer funds from inactive accounts into a favored account and then 'legitimately' withdrawing the funds.

The definition of computer-related crime should be based on the problem that needs to be solved. The problem addressed is twofold: how to reduce the incidence of any type of crime in which a knowledge of computer technology is needed to understand the intentional acts that result in losses and how to successfully prosecute the perpetrators. Whereas this is now predominantly a white-collar crime, the criminal justice and business communities must be prepared to deal with any illegal acts based on an understanding of computer technology. A study of 669 reported cases of computer abuse over the past 8 years has revealed that computers are involved in an increasing number of crimes of all types except murder and person-to-person street crimes. [1] The proliferation and use of personal small computers make even the latter crimes subject at least to the indirect involvement of computer technology.

The broadest definition of computer crime is called for. The term "crime" is used here (as is usual) as a convenience to mean "alleged crime" because no harmful or antisocial act is a crime until a court declares it so by convicting a party for violating a law. Three terms have been used to describe the subject: "computer abuse," "computer crime," and "computer-related crime." Computer abuse identifies the broad range of intentional acts from which something can be learned to make organizations that use computers more secure. [2] Computer abuse is any intentional act involving a computer where one or more perpetrators made or could have made gain and one or more victims suffered or could have suffered a loss.

Computer crime is a common term used to identify illegal computer abuse; however, it implies direct involvement of computers in committing a crime. Therefore, we adopt the term computer-related crime that conveys the broader meaning of <u>any illegal act for which knowledge of computer technology is essential for successful prosecution</u>. This definition is based on the scope and nature of the particular problem being addressed. The crimes and alleged crimes may involve computers not only actively but also passively when usable evidence of the acts reside in computer stored form. The victims and potential victims include all organizations and persons who use or are affected by computer and data communication systems. People about whom data are stored and processed in computers also are included.

Computer-related crime goes far beyond business, white-collar, or economic crime. It could include violent crime that destroys computers or their content or jeopardizes human life and well-being because they are dependent on the correct functioning of computers controlling sensitive processes.

Computers play four roles in crime:

- Object--Cases include destruction of computers or of data or programs contained in them or supportive facilities and resources such as air conditioning equipment and electrical power, that allow them to function.

- Subject--A computer can be the site or environment of a crime or the source of or reason for unique forms and kinds of assets.

- Instrument--Some types and methods of crime are complex enough to require the use of a computer as a tool or instrument. A computer can be used actively such as in automatically scanning telephone codes to make unauthorized use of a telephone system. It could also be used passively to simulate a general ledger in the planning and control of a continuing financial embezzlement.

- Symbol--A computer can be used as a symbol for intimidation or deception. This could involve the false advertising of nonexistent services, such as in dating bureaus.

All known and reported cases of computer-related crime involve one or more of these four roles.

The dimensions of the definition of computer-related crime become a problem in some cases. If a computer is stolen in a simple theft where based on all circumstances it could have been a washing machine or milling machine and made no difference, then a knowledge of computer technology is not necessary, and it would not be a computer-related crime. However, if knowledge of computer technology is necessary to determine the value of the article taken, the nature of possible damage done in the taking, or the intended use by the thief is at issue, then it would be a computer-related crime. To illustrate, if an individual makes a telephone call to a bank funds transfer department and fraudulently requests a transfer of $10 million to his account in a bank in Zurich, two possibilities occur. If the clerk who received the call was deceived and keyed the transfer into a computer terminal, the funds transfer would not be a computer-related crime. No fraudulent act was related directly to a computer, and no special knowledge of computer technology would be required. However, if the clerk was in collusion with the caller, the fraudulent act would include the entry of data at the terminal and would be a computer-related crime. Knowledge of computer technology would be necessary to understand the terminal usage and protocol. These examples indicate the possibilities of rational conclusions in defining computer-related crime. However, more practical

considerations should not make such explicit and absolute decisions necessary. If any information in this manual is useful for dealing with any kind of crime, its use should be encouraged. Finally, as the criminal justice community has begun to understand from experience the involvement of computers across all types of crime, the definition has broadened. It is expected that the results of efforts funded by LEAA will establish a consensus on a broad definition of computer-related crime to cover the current and anticipated experience.

C. A CLASSIFICATION OF COMPUTER-RELATED CRIME

A classification of computer-related crime is based on a variety of lists and models from several sources to produce standards for categorization. The classification goes beyond white-collar crimes because, as stated above, computers have been found to be involved in robbery, larceny, extortion, espionage, and sabotage.

Senator Abraham Ribicoff's recent Senate Bill (S240) to amend Title 18 of the U.S. Criminal Code (see Appendix A) is an omnibus crime bill making crimes of unauthorized acts in, around, and with computer and telecommunication systems. He identifies four main categories of computer-related crime: [3]

- The introduction of fraudulent records or data into a computer system.
- Unauthorized use of computer related facilities.
- The alteration or destruction of information or files.
- The stealing, whether by electronic means or otherwise of money, financial instruments, property, services, or valuable data.

A computer abuse study has identified categories in several dimensions: [2]

- Categorized by type of loss: physical damage and destruction from vandalism, intellectual property, direct financial gain and use of services.
- Categorized by the role played by computers: object of attack, unique environment and forms of assets produced, instrument, and symbol.
- Categorized by type of act relative to data, computer programs, and services: modification, destruction, disclosure, and use of services.
- Categorized by type of crime: fraud, theft, robbery, larceny, arson, embezzlement, extortion, conspiracy, sabotage, and espionage.

- Categorized by modi operandi: physical attacks, false data entry, superzapping, impersonation, wire tapping, Piggybacking, social engineering, scavenging, Trojan horse attacks, trap door use, asynchronous attacks, salami techniques, data leakage, logic bombs, and simulation.

These classifications can be developed into a set of complete, detailed descriptions and models of computer related crime. They can be useful for a variety of research and practical purposes in investigation and prosecution of computer-related crime.

D. HISTORY OF COMPUTER-RELATED CRIME

Computer abuse started with the emergence of computer technology in the late 1940s. As the number of people in the computer field began to increase, the facet of human nature of doing harm to society for personal gain took hold as it does with any segment of the human population; the problem of crime became especially acute as computer technology proliferated into sensitive areas in society. This occurred first in military systems and then in engineering, science, and finally business applications.

The first recorded computer abuse occurred in 1958 [2]. The first federally prosecuted computer-related crime, identified as such, was the alteration of bank records by computer in Minneapolis in 1966. Table 1 is a computer-produced index of collected cases of computer abuse. [4] Some fraction of the 669 cases can be considered to be computer-related crimes (where illegal activities have been proved).

Pursuit of the study of computer-related crime and computer abuse has been controversial. In 1970, a number of researchers concluded that the problem was merely a small part of the effect of technology on society and was not worthy of specific, explicit research. The increase in substantial losses associated with intentional acts involving computers proved the fallacy of this view. The explicit identification of computer-related crime as a subject for research and development of preventative measures in criminal justice suffered a similar fate in the mid-1970s. Researchers argued that computers should not be the focus in a study of various types of crime. They believed the involvement of computers should be subordinate to the study of each specific type of crime, both manual and automated. The uniqueness of characteristics of computer-related crime across all the different types of crime was not considered sufficient to warrant explicit research.

The formal study of computer abuse was started in 1971. The first national conference on computer abuse and a comprehensive report were completed in 1973. [2] Since then, many reports, papers, journal articles, and books have been published describing the research. [5]

The interest of the criminal justice community began in response to increasing numbers of cases and action by criminal justice

Table 1

COMPUTER ABUSE CASES

04/13/79

INCIDENCE AND LOSS BY TYPE OF CRIME (YEARLY)

YEAR	TYPE 1 PHYSICAL DESTRUCTION			TYPE 2 INTELLECTUAL PROPERTY DECEPTION AND TAKING			TYPE 3 FINANCIAL DECEPTION AND TAKING			TYPE 4 UNAUTHORIZED USE OF SERVICES			ALL TYPES		
	NO. OF CASES; % OF TOTAL	KNOWN LOSSES FOR TYPE 1	AV. LOSS PER CASE, TYPE 1	NO. OF CASES; % OF TOTAL	KNOWN LOSSES FOR TYPE 2	AV. LOSS PER CASE, TYPE 2	NO. OF CASES; % OF TOTAL	KNOWN LOSSES FOR TYPE 3	AV. LOSS PER CASE, TYPE 3	NO. OF CASES; % OF TOTAL	KNOWN LOSSES FOR TYPE 4	AV. LOSS PER CASE, TYPE 4	TOTAL CASES	TOTAL KNOWN LOSSES	AVERAGE LOSS
1958	- -	-	-	- -	-	-	1 0%	<1	<1	- -	-	-	1		
1959	- -	-	-	- -	-	-	1 0%	278	278	- -	-	-	1	278	277
1962	2 0%	-	-	- -	-	-	- -	-	-	- -	-	-	2	-	-
1963	1 50%	2,000	2,000	- -	-	-	1 50%	61	61	- -	-	-	2	2,061	1,043
1964	1 17%	-	-	2 33%	2,500	2,500	3 50%	100	100	- -	-	-	6	2,600	1,300
1965	- -	-	-	1 13%	-	-	4 50%	126	63	3 38%	-	-	8	126	63
1966	1 33%	<1	<1	- -	-	-	2 67%	26	14	- -	-	-	3	26	9
1967	2 50%	<1	<1	- -	-	-	- -	-	-	2 50%	10	10	4	10	5
1968	1 8%	-	-	3 25%	7,203	3,602	6 50%	5,251	1,313	2 17%	-	-	12	12,454	2,075
1969	4 20%	2,000	2,000	8 40%	1,003	334	4 20%	6	2	4 20%	2	2	20	3,011	376
1970	8 21%	3,600	900	6 16%	6,849	1,369	13 34%	8,910	810	11 29%	-	-	38	19,353	967
1971	7 12%	-	-	20 34%	9,844	1,641	24 41%	5,943	540	8 14%	351	175	59	16,137	849
1972	17 23%	11,146	2,230	19 26%	160	30	19 26%	3,090	257	18 25%	107	21	73	14,524	518
1973	10 13%	4	2	26 35%	26,782	2,435	28 37%	206,274	11,460	11 15%	7	1	75	233,066	6,474
1974	7 10%	2,010	1,005	20 27%	2,197	439	34 47%	3,952	158	12 16%	3	3	73	8,162	247
1975	5 6%	115	58	21 25%	91,670	13,096	49 58%	6,513	176	9 11%	14	5	84	98,312	2,006
1976	5 8%	1,110	370	19 32%	49,465	7,066	30 51%	2,026	78	5 8%	-	-	59	52,601	1,461
1977	14 16%	2,252	322	16 18%	17,946	2,991	44 51%	47,501	1,319	13 15%	154	77	87	67,853	1,330
1978	10 24%	2,523	841	13 31%	300	50	17 40%	12,384	826	2 5%	-	-	42	15,207	633
1979	2 10%	-	-	11 55%	-	-	4 20%	200	200	3 15%	-	-	20	200	200
TOTAL	97 14%	26,761	836	185 28%	215,932	3,322	284 42%	302,661	1,462	103 15%	646	32	669	546,001	1,685

CASES: TOTAL KNOWN CASES OF THIS TYPE IN YEAR, WHETHER OR NOT LOSS IS KNOWN
KNOWN LOSSES: IN THOUSANDS OF DOLLARS
AV. LOSS: AVERAGE FOR CASES WHERE LOSS IS KNOWN

organizations, including the FBI Academy, Criminal Justice Conferences on white-collar and organized crime, National District Attorneys Association Economic Crime Project, local FBI offices, and the National College of District Attorneys. In 1976, the FBI established for its agents a 4-week training course in investigation of computer-related crime and another for other agencies in 1978.

In 1976, as a result of the increasing frequency of cases, Senator Abraham Ribicoff and his U.S. Senate Government Affairs Committee became aware of computer-related crime and the inadequacy of federal criminal law to deal with it. The committee produced two reports on its research [U.S. Senate 1976, 1977], [6, 7] and Senator Ribicoff introduced the first Federal Systems Protection Act Bill in June 1977. As the result of U.S. Justice Department comments and hearings on the bill in June 1978 [8], the Bill was revised and a new bill, S240, was introduced into the current Congress (see Appendix A). On the state level, Florida, Michigan, Colorado, Rhode Island, and Arizona have computer-related crime laws based on the first Ribicoff bill. Current state legislation on computer-related crime is provided in Appendix B and proposed legislation in Appendix C.

Recent research has produced a number of publications on computer-related crime. Among them are: "Operational Guide to White-Collar Crime Enforcement, On the Investigation of Computer Crime" [9]; "Manual for Prosecution of Computer-Related Crime" [10]; and "Computer Crime Investigation Manual," published commercially. [11]

Computer-related crime has been portrayed fictionally in several novels [12, 13], motion pictures, and television dramas. Two comic strips, Dick Tracy and Steve Roper, have depicted fictional stories. The computer-related crime aspects of a massive insurance fraud were dramatized by the British Broadcasting System. NBC TV News and CBS 60 Minutes have had special segments. Several nonfiction trade books have been published, and articles have appeared in all major magazines and newspapers. Unfortunately, the public interest and sensationalism associated with computer-related crime has made folk heroes of the perpetrators and caused significant embarrassment to the victims. Prosecutors have sometimes benefited from the visibility of their cases and the high conviction rate.

E. INVESTIGATION AND PROSECUTION EXPERIENCE

Extensive field work preceded the writing of this manual. In particular, several weeks were spent interviewing 44 prosecutors and investigators in the Los Angeles District Attorney's office and several prosecutors in offices in New York City and Philadelphia. Their experiences in prosecuting computer-related crime and more than 50 cases were documented. A questionnaire survey of 49 prosecutors was also conducted. [14] The information obtained has been used as the basis for parts of this manual.

The initial reaction to inquiries about deputy district attorneys' (DDAs) experiences with computer-related crime is that "we have had no computer-related crime cases." Further discussion usually indicated that they have had several crime cases in which computers had been involved to a significant extent, but DDAs had failed to classify them as computer-related crimes. There was general agreement that there will be an increasing number of computer-related crimes. Moreover, the defendant and his defense attorney understand the technical aspects of the computer involved in the case; therefore, it is important that the prosecutor also understand them.

F. COMPUTER-RELATED CRIME METHODS AND DETECTION

Investigators and prosecutors should deal with computer-related crime as much as possible in the context of their experience with other, more traditional, crime. However, when computer technology plays a key role that cannot be avoided, a thorough understanding of criminal methods involving computers is essential. In addition, being aware of the types of people who have the skills and knowledge to use these methods, likely evidence of their use and detection methods can be most helpful.

This section describes 12 computer-related crime methods in which computers play a key role. Although several of the methods are far more complex than the nonexpert will understand in detail, these brief descriptions will aid investigators and prosecutors to comprehend sufficiently to interact with technologists who can provide the necessary expertise to deal with them. Most technologically sophisticated computer-related crimes will use one or more of these methods. However, no matter how complex the methods, the crimes will still fit into the categories familiar to the prosecutor. For an explanation of the technical terms used in this discussion the reader is referred to Section VI, "Overview of Computer Technology," the glossary, or the index.

Like most aspects of computer technology, a jargon describing the now classical methods of computer-related crime has developed. These are the technical methods for some of the more sophisticated and automated computer-related crimes. The results are modification, disclosure (taking), destruction, and use or denial of use of services, computer equipment, computer programs, or data in computer systems. Depending on the meaning of the data, kinds of services, or purpose of the programs, the acts range over many known types of crime. The methods, possible types of perpetrators, likely evidence of their use, and detection are described below.

1. Data Diddling

This is the simplest, safest, and most common method used in computer-related crime. It involves changing data before or during their input to computers. The changing can be done by anybody associated with or having access to the processes of creating,

recording, transporting, encoding, examining, checking, converting, and transforming data that ultimately enter a computer. Examples are forging or counterfeiting documents; exchanging valid computer tapes, cards, or disks with prepared replacements; source entry violations; punching extra holes or plugging holes in cards; and neutralizing or avoiding manual controls.

Data are normally protected by manual methods, and once data are in the computer, they can be automatically validated and verified. Manual controls include maker-checker-signer roles for trusted people with separation of responsibilities or dual responsibilities that force collusion to perpetrate fraudulent acts. Batch control totals can be manually calculated and compared in the computer with matching computer-produced batch control totals. In this method, data are batched into small groups, and data are added together to produce a sum that is the control total. Another common control is the use of check digits or characters imbedded in the data based on various characteristics of each field of data (e.g., odd or even number indicators or hash totals). Sequence numbers and time of arrival can be associated with data and checked to ensure that data have not been removed or reordered. Large volumes of data can be checked by using utility or special-purpose programs in a computer. Evidence of data diddling is discovered data that do not correctly represent data as found at sources, lack equality with redundant or duplicate data, do not match earlier forms of data by reversing the manual processes that have been carried out, control totals or check digits that do not check nor meet validation and verification tests in the computer.

A typical example is the case of a timekeeping clerk who filled out data forms of hours worked by 300 employees in a department of a railroad company. He noticed that all data on the forms were entered into the timekeeping and payroll system on the computer included both the name and the employee number of each worker. However, the computer used only employee numbers for processing and even for looking up employee names and addresses to print on payroll checks. He also noticed that outside the computer all manual processing and control was based only on employee names, because nobody identified people by their numbers. He took advantage of this dichotomy of controls by filling out forms for overtime hours worked and using names of employees who frequently worked overtime but entering his own employee number. This was never discovered, and his income was increased by several thousand dollars every year until by chance an auditor examining W-2 federal income forms noticed the unusually high annual income of the clerk. An examination of the timekeeping computer files and recent timekeeping data forms and a discussion with the clerk's supervisor revealed the source of the increased income. The clerk was confronted with the evidence and admitted his fraudulent activities. The clerk's activities were not sophisticated but surely represent a data diddling computer-related crime. Well-designed timekeeping and payroll systems use the first few letters of employees' names appended to their identification numbers to reduce the likelihood of this type of crime.

Potential data diddling perpetrators are employed in different kinds of occupations. Table 2 summarizes these potential perpetrations, the methods of detecting data diddling, and the sources of evidence.

Table 2
DETECTION OF DATA DIDDLING

Potential Perpetrators	Methods of Detection	Evidence
Transaction participants	Data comparison	Data documents Source Transactions Computer-readable
Data preparers	Document validation	
Source data supplies	Manual controls instrumentation analysis	Computer data media Tapes Cards Disks Storage modules
Nonparticipants with access	Computer validation and verification exception	
	Reports analysis	Manual logs, journals, and exception reports
	Computer output	
	Integrity tests	Incorrect computer output

2. Trojan Horse

The Trojan horse method is the covert placement of computer instructions in a program so that the computer will perform unauthorized functions but usually still will allow the program to perform its intended purposes. This is the most common method in computer program-based frauds and sabotage. Instructions may be placed in production computer programs so that they will be executed in the protected or restricted domain of the program and have access to all of the data files that are assigned for exclusive use of the program. Programs are usually constructed loosely enough to allow space to be found or created for inserting the instructions.

There are no practical methods of preventing and detecting Trojan horse methods if the perpetrator is sufficiently clever. A typical business application program can consist of over 100,000 computer instructions and data. The Trojan horse can also be concealed among up to 5 or 6 millions of instructions in the operating system and commonly used utility programs where it waits for execution of the target application program, inserts extra instructions in it for a few milliseconds of execution time, and removes them with no remaining evidence. Even if it is discovered, there is no indication of who may

have done it except to narrow the search to those programmers who have the necessary skills, knowledge, and access among employees, former employees, contract programmers, consultants, or employees of the computer or software suppliers. However, the perpetrator may be continuing to benefit from his acts by converting them to economic gain directly or through accomplices. If the conversion to assets can be determined and traced, there is a chance of apprehension using this method.

A suspected Trojan horse might be discovered by comparing a copy of the operational program under suspicion with a master or other copy known to be free of unauthorized changes. Backup copies of production programs are routinely kept in safe storage, but smart perpetrators will make duplicate changes in them. Also programs are frequently changed without changing the backup copies, thereby making comparison difficult. Utility programs are usually available to perform comparisons of large programs, but their integrity and the computer system on which they are executed must be assured. This should be done only by qualified and trusted experts.

A Trojan horse might also be detected by testing the suspect program with data and under conditions that might cause the exposure of the purpose of the Trojan horse. However, the probability of success is low unless exact conditions for discovery are known. This may prove the existance of the Trojan horse, but usually will not determine its location. A Trojan horse may also reside in the source language version or only in the object form and may be inserted in the object form each time it is assembled or compiled--e.g., as the result of another Trojan horse in the assembler or compiler.

The methods for detecting Trojan horse frauds are summarized in Table 3. The table also lists the occupations of potential perpetrators and the sources of evidence fo Trojan horse crime.

Table 3

DETECTION OF TROJAN HORSE CRIMES

Potential Perpetrators	Methods of Detection	Evidence
Programmers having detailed knowledge of a suspected part of a program and its purpose and access to it	Program code comparison	Unexpected results of program execution
	Testing of suspect program	
	Tracing of possible gain from the act	Foreign code found in a suspect program
Employees Contract programmers Vendor's programmers Users of the computer		

3. Salami Techniques

An automated form of crime involving the theft of small amounts of assets from a large number of sources is identified as a salami technique (taking small slices without noticeably reducing the whole). For example, in a banking system the demand deposit accounting system for checking accounts could be changed (using the Trojan horse method) to randomly reduce a few hundred accounts by 10 cents or 15 cents by transferring the money to a favored account where it can be legitimately withdrawn through normal methods. No controls are violated because the money is not removed from the system of accounts. Instead, a small fraction of it is merely rearranged. The success of the fraud is based on the idea that each checking account customer looses so little that it is of little consequence. Many variations are possible. The assets may be an inventory of products or services as well as money.

One salami method in a financial system is known as the "round down" fraud. The round down fraud requires a computer system application where large numbers of financial accounts are processed. The processing must involve the multiplication of dollar amounts by numbers--such as in interest rate calculations. This arithmetic results in products that contain fractions of the smallest denomination of currency, such as the cent in the United States. For example, a savings account in a bank may have a balance of $15.86. Applying the 2.6% interest rate results in adding $0.41236 ($15.86 x .026) to the balance for a new balance of $16.27236. However, because the balance is to be retained only to the nearest cent, it is rounded down to $16.27, leaving $0.00236. What is to be done with this remainder? The interest calculation for the next account in the program sequence might be the following: $425.34 x 0.026 = $11.05884. This would result in a new balance of $436.39884 that must be rounded up to $436.40, leaving a deficit or negative remainder of $0.00116, usually placed in parenthesis to show its negative value ($0.00116).

The net effect of rounding in both these accounts, rounding down to the calculated cent in the first and adding 1 cent in the second, leaves both accounts accurate to the nearest cent and a remainder of $0.0012 ($0.00236 - $0.00116). This remainder is then carried to the next account calculation, and so on. As the calculations continue, if the running or accumulating remainder goes above 1 cent, positive or negative, the last account is adjusted to return the remainder to an amount less than 1 cent. This results in a few accounts receiving 1 cent more or less than the correct rounded values, but the totals for all accounts remain in balance.

This is where the creative computer programmer can engage in some trickery to accumulate for himself a fancy bit of change and still show a balanced set of accounts that defies discovery by the auditor. He merely changes the rules slightly in the program by accumulating the rounded down remainders in his own account rather than distributing them to the other accounts as they build up.

Using a larger number of accounts shows how this is done. First, if rounded down correctly, it would be as shown in Table 4. [15] The interest rate applied to the total of all accounts, $3,294.26, results in a new total balance of $3,379.91 ($3,294.26 x 1.026) and a remainder of $0.00076 when the new total balance is rounded. This is calculated by the program as verification that the arithmetic performed account by account is correct. However, note that several accounts (those marked with an asterisk) have 1 cent more or less than they should have.

Now suppose the programmer writes the program to accumulate the round amounts into his own account, the last account in the list. The calculations will be as shown in Table 5. The totals are the same as before and the verification shows no tinkering. However, now the new balances of some accounts are 1 cent less, but none are 1 cent more as in the previous example. Those extra cents have been accumulated and all added to the programmer's account (the last account in the list) rather than to the accounts where the adjusted remainder exceeded 1 cent.

Table 4
EXAMPLE OF ROUNDED DOWN ACCOUNTS

Old Balance	New Balance	Rounded New Balance	Remainder	Accumulating Remainder
$ 15.86	$ 16.27236	$ 16.27	$ 0.00236	$ 0.00236
425.34	436.39884	436.40	(0.00116)	0.00120
221.75	227.51550	227.52	(0.00450)	(0.00330)
18.68	19.16568	19.17	(0.00432)	(0.00762)
o 564.44	579.11544	~~579.12~~	(0.00456)	(0.01218)
		579.11		(0.00218)
61.31	62.90406	62.90	0.00406	0.00188
101.32	103.95432	103.95	0.00432	0.00620
o 77.11	79.11486	~~79.11~~	0.00486	0.01106
		79.12		0.00106
457.12	469.00512	469.01	(0.00488)	(0.00382)
111.35	114.24510	114.25	(0.00490)	(0.00872)
o 446.36	457.96536	~~457.97~~	(0.00464)	(0.01336)
		457.96		(0.00336)
88.68	90.98568	90.99	(0.00432)	(0.00768)
o 14.44	14.81544	~~14.82~~	(0.00456)	(0.01224)
		14.81		(0.00224)
83.27	85.43502	85.44	(0.00498)	(0.00722)
127.49	130.80474	130.80	0.00474	(0.00248)
331.32	339.93432	339.93	0.00432	0.00184
37.11	38.07486	38.07	0.00486	0.00670
o 111.31	114.20406	~~114.20~~	0.00406	0.01076
		114.21		0.00076
---		---		
$3294.26	Total	$3379.91		

Table 5

EXAMPLE OF ROUNDED DOWN ACCOUNTS CONVERTED TO PROGRAMMER'S ACCOUNT

Old Balance	New Balance	Rounded New Balance	Remainder	Accumulating Remainder	Programmer's Remainder
$ 15.86	$ 16.27236	$ 16.27	$ 0.00236	$ 0.00000	$0.00236
425.34	436.39884	436.40	(0.00116)	(0.00116)	0.00236
221.75	227.51550	227.52	(0.00450)	(0.00566)	0.00236
18.68	19.16568	19.17	(0.00998)	(0.00998)	0.00236
o 564.44	579.11544	~~579.12~~	(0.00456)	(0.01454)	0.00236
		579.11		(0.00454)	
61.31	62.90406	62.90	0.00406	(0.00454)	0.00642
101.32	103.95432	103.95	0.00432	(0.00454)	0.01074
77.11	79.11486	79.11	0.00486	(0.00454)	0.01560
457.12	469.00512	469.01	(0.00488)	(0.00942)	0.01560
o 111.35	114.24510	~~114.25~~	(0.00490)	(0.01432)	0.01560
		114.24		(0.00432)	
446.36	457.96536	457.97	(0.00464)	(0.00896)	0.01560
o 88.68	90.98568	90.99	(0.00432)	(0.01328)	0.01560
		90.98		(0.00328)	
14.44	14.81544	14.82	(0.00456)	(0.00784)	0.01560
o 83.27	85.43502	~~85.44~~	(0.00498)	(0.01282)	0.01560
		85.43		(0.00282)	
127.49	130.80474	130.80	0.00474	(0.00282)	0.02034
331.32	339.93432	339.93	0.00432	(0.00282)	0.02466
37.11	38.07486	38.07	0.00486	(0.00282)	0.02952
o 111.31	114.20406	~~114.20~~	0.00406	(0.00282)	0.03358
		114.23		0.00076	0.00000
---		---			
$3.294.26	Total	$3379.91			

Clearly, if there were 180,000 accounts instead of the 18 accounts in this example, the programmer could have made a tidy profit of $300 ($0.03 x 10,000). This could result in a significant fraud over several years.

There are only two ways that the auditor might discover this fraud. He could check the instructions in the program, or he could recalculate the interest for the programmer's account after the program had been executed by the computer. A clever programmer could easily disguise the instructions causing the fraudulent calculations in the program in a number of ways. However, this would probably be unnecessary because an auditor or anybody else would probably not wade step by step through a program so long as use of the program showed no irregularities.

This program method would show no irregularities unless the programmer's account were audited. It is unlikely that his account--one account among 180,000--would be audited. Besides, the programmer could have opened the account using a fictitious name or the name of an accomplice. He could also occasionally change to other accounts to reduce further the possibility of detection.

Experienced accountants and auditors indicate that the round down fraud technique has been known for many years, even before the use of computers. They say that a good auditor will look for this type of fraud by checking for deviations from the standard accounting method for rounding calculations.

Salami acts are usually not fully discoverable within obtainable expenditures for investigation. Victims have usually lost so little individually that they are unwilling to expend much effort to solve the case. Specialized detection routines can be built into the suspect program, or snapshot storage dump listings could be obtained at crucial times in suspect program production runs. If the salami acts are taking identifiable amounts, these can be traced, but a smart perpetrator will randomly vary the amounts or accounts debited and credited.

The actions and life styles of the few people and their associates who have the skills, knowledge, and access to perform salami acts can be closely watched for aberrations or deviations from normal. This could be successful because real-time actions are usually required to convert the results to obtainable gain. The perpetrator or his accomplice will usually withdraw the money from the accounts in which it accumulates in legitimate ways. Records will show an imbalance between the deposit and withdrawal transactions, but all accounts would have to be balanced relative to all transactions over a significant period of time. This is a monumental and expensive task.

Many financial institutions require employees to use their financial services and make it attractive for them to do so. Employees' accounts are more completely and carefully audited than others. This usually forces the salami perpetrators to open accounts under assumed names or arrange for accomplices to do it. Investigation of suspected salami frauds might be more successful through concentrating on the actions of possible suspects rather than relying on technical methods of discovery.

Table 6 lists the methods of detecting the use of salami techniques. The table also lists potential perpetrators and source of evidence of the use of the technique.

Table 6
DETECTION OF SALAMI TECHNIQUES

Potential Perpetrators	Methods of Detection	Evidence
Financial system programmers	Detail data analysis	Many small financial losses
Employees Former employees Contract programmers Vendors' programmers	Program comparison	Unsupported account buildups
	Transaction audits	Trojan horse code changed or unusual
	Observation of financial activities of possible suspects	personal financial practices of possible suspects

4. Superzapping

Superzapping derives its name from superzap, a macro/utility program used in most IBM computer centers as a systems tool. Any computer center that has a secure computer operating mode needs a "break glass in case of emergency" computer program that will bypass all controls to modify or disclose any of the contents of the computer. Computers sometimes stop, malfunction or enter a state that cannot be overcome by normal recovery or restart procedures. Computers also perform unexpectedly and need attention that normal access methods do not allow. In such cases, a universal access program is needed. This is similar in one way to a master key to be used if all other keys are lost or locked in the enclosure they were meant to open.

Utility programs such as superzap are powerful and dangerous tools in the wrong hands. They are normally used only by systems programmers and computer operators who maintain computer operating systems. They should be kept secure from unauthorized use. However, they are often placed in program libraries where they can be used by any programmer or operator who knows of their presence and how to use them.

A classic example of superzapping resulting in a $128,000 loss occurred in a bank in New Jersey. [15] The manager of computer operations was using a superzap program to make changes to account balances to correct errors as directed by management. The regular error correction process was not working correctly because the demand-deposit accounting system had become obsolete and error-ridden as a result of inattention in a computer changeover. The operations manager discovered how easy it was to make changes without the usual controls or journal records, and he made changes transferring money to three friends' accounts. They engaged in the fraud long enough for a customer to find a shortage: quick action in response to the customer's complaint resulted in indictment and conviction of the perpetrators. The use of the superzap program without leaving any evidence of changes to the data files made discovery of the fraud through technical means highly unlikely.

Unauthorized use of superzap programs can result in changes to data files that are normally updated only by production programs. There usually are few if any controls that would detect changes in the data files from previous runs. Application programmers do not anticipate this type of fraud; their universe of concern is limited to the application program and its interaction with data files. Therefore, the detection of fraud will result only when the recipients of regular computer output reports from the production program notify management that a discrepancy seems to have occurred. Computer managers will often conclude that the evidence indicates data entry errors, because it would not be a characteristic computer or program error. Considerable time can be wasted from searching in the wrong areas. When it is concluded that unauthorized file changes have occurred independent of the application program associated with the file, a search of all computer usage journals might reveal the use of a superzap program, but this is unlikely if the perpetrator anticipates this. Occasionally, there may be a record of a request to have the file placed on-line in the computer system if it is not normally in that mode. Otherwise, the changes would have to occur when the production program using the file is being run or just before or after it is run. This is the most likely time of the act.

Detection of the superzap acts may be possible by comparing the current file with father and grandfather copies of the file where no updates exist to account for suspicious changes. Table 7 summarizes the potential perpetrators, methods of detection, and sources of evidence in superzapping crime.

Table 7

DETECTION OF SUPERZAPPING CRIME

Potential Perpetrators	Method of Detection	Evidence
Programmers with access to superzap programs and computer access to use them	Comparison of files with historical copies	Output report discrepancies
	Discrepancies noted by recipients of output reports	Undocumented transactions
Computer operations staff with applications knowledge	Examination of computer usage journals	Computer usage or file request journals

5. Trap Doors

In the development of large application and computer operating systems, it is the practice of programmers to insert debugging aids that provide breaks in the code for insertion of additional code and intermediate output capabilities. The design of computer operating systems attempts to prevent both access to them and insertion of code or modification of code. Consequently, system programmers will sometimes insert code that allows compromise of these requirements during the debugging phases of program development and later when the system is being maintained and improved. These facilities are referred to as trap doors. Normally, trap doors are eliminated in the final editing but sometimes they are overlooked or purposely left in to facilitate ease of making future access and modification. In addition, some unscrupulous programmers may purposely introduce trap doors for later compromising of computer programs. Designers of large complex programs may also introduce trap doors inadvertently through weaknesses in design logic.

Trap doors may also be introduced in the electronic circuity of computers. For example, not all of the combinations of codes may be assigned to instructions found in the computer and documented in the programming manuals. When these unspecified commands are used, the circuitry may cause the execution of unanticipated combinations of functions that allow compromise of the computer system.

During the use and maintenance of computer programs and computer circuitry, ingenious programmers invariably discover some of these weaknesses and take advantage of them for useful and innocuous purposes. However, the trap doors may also be used for unauthorized, malicious purposes as well. Functions that can be performed by computer programs and computers that are not in the specifications are often referred to as negative specifications. It is difficult enough for designers and implementers to make programs and computers function according to specifications and to prove that they perform according to specifications. It is currently not possible to prove that a computer system does not perform functions that it is not specified to perform.

Research is continuing on a high-priority basis to develop methods of proving the correctness of computer programs and computers according to complete and consistent specifications. However, it is anticipated that it will be many years before commercially available computers and computer programs can be proved correct. Therefore, trap doors continue to exist, and there is never any guarantee that they have all been found and corrected.

In one computer-related crime, a systems programmer discovered a trap door in a FORTRAN programming language compiler. The trap door allowed the programmer writing in the FORTRAN (FORmula TRANslation) language to transfer control from his FORTRAN program into a region of storage used for data. This caused the computer to execute computer instructions formed by the data and provided a means of executing

program code secretly by inputting data in the form of computer instructions each time the FORTAN program was run. This occurred in a commercial time-sharing computer service. The systems programmer in collusion with a user of the time-sharing service was able to use large amounts of computer time free of charge and obtain data and programs of other time-sharing users. In another case, several automative engineers in Detroit discovered a trap door in a commercial time-sharing service in Florida that allowed them to search uninhibitedly for privileged passwords. They discovered the password of the president of the time-sharing company and were able to obtain copies of trade-secret computer programs that they proceeded to use free of charge. In both of these cases the perpetrators were discovered accidentally. It was never determined how many other users were taking advantage of the trap doors.

There is no direct technical method for the discovery of trap doors. However, when the nature of a suspected trap door is sufficiently determined, tests of varying degrees of complexity can be performed to discover hidden functions used for malicious purposes. This requires the expertise of systems programmers and knowledgeable application programmers. Large amounts of computer services and time could be wasted by people without sufficient expertise attempting to discover trap door usage. Investigators should always seek out the most highly qualified experts for the particular computer system or computer application under suspicion.

It is wise for the investigator always to assume that the computer system and computer programs are never sufficiently secure from intentional, technical compromise. However, these intentional acts usually require the expertise of only the very few technologists who have the skills, knowledge, and access to perpetrate them. Table 8 lists the potential perpetrators, methods of detection, and sources of evidence of the use of the trap door technique.

Table 8

DETECTION OF TRAP DOOR CRIMES

Potential Perpetrators	Methods of Detection	Evidence
Systems programmers	Exhaustive testing	Computer output reports that indicate that a computer system performs outside of its specifications
Expert application programmers	Comparison of specification to performance	
	Specific testing based on evidence	

6. Logic Bombs

A logic bomb is a computer program executed at appropriate or periodic times in a computer system that determines conditions or states of the computer that facilitate the perpetration of an unauthorized, malicious act. For example, in one case, secret computer instructions were inserted (a Trojan horse) in the computer operating system where they were executed periodically. [15] The instructions would test the year, date and time of day clock in the computer so that on a specified day of the year 2 years later at 3:00 P.M. the time bomb, a type of logic bomb, would go off and trigger the printout of a confession of a crime on all of the 300 computer terminals on-line at that time and then would cause the system to crash. This was timed so that the perpetrator would be geographically a long distance from the computer and its users. In another case, a payroll system programmer put a logic bomb in the personnel system so that if his name was ever removed from the personnel file, indicating termination of employment, secret code would have caused the entire personnel file to be erased.

A logic bomb can be programmed to trigger an act based on any specified condition or data that may occur or be introduced. Logic bombs are usually placed in the computer system using the Trojan horse technique. Methods to discover logic bombs in a computer system would be the same as for Trojan horses. Table 9 summarizes the potential perpetrators, methods of detection, and kinds of evidence of logic bombs.

Table 9

DETECTION OF LOGIC BOMBS

Potential Perpetrators	Methods of Detection	Evidence
Programmers having detailed knowledge of a suspected part of a program and its purpose and access to it	Program code comparisons	Unexpected results of program execution
	Testing of suspect program	Foreign code found in a suspect program
Employees Contract programmers Vendor's programmers Users of the computer	Tracing of possible gain from the act	

7. Asynchronous Attacks

Asynchronous attack techniques take advantage of the asynchronous functioning of a computer operating system. Most computer operating systems function asynchronously based on the services that must be performed for the various computer programs in execution in the computer

system. For example, several jobs may simultaneously call for output reports to be produced. The operating system stores these requests and, as resources become available, performs them in the order in which resources are available to fit the request or according to an overriding priority indication. Therefore, rather than executing requests in the order they are received, the system performs them asynchronously based on resources available.

There are highly sophisticated methods of confusing the operating system to allow it to violate the isolation of one job from another. For example, in a large application program that runs for a long period of time, it is customary for it to have checkpoint restarts. These allow the computer operator to set a switch manually to stop the program at a specified intermediate stopping point from which it may be restarted at a later time in an orderly manner without losing data. This requires the operating system to save the copy of the computer program and data in their current state at the checkpoint. The operating system must also save a number of system parameters that describe the mode and security level of the program at the time of the stop. It might be possible for a programmer or computer operator to gain access to the checkpoint restart copy of the program, data, and system parameters. He could change the system parameters such that on restart the program would function at a higher priority security level or privileged level in the computer and thereby give the program unauthorized access to data, other programs, or the operating system. Note that checkpoint restart actions are usually well documented in the computer console log.

Even more complex methods of attack could be used besides the one described in this simple example. However, the technology is too complex to present here. The investigator should be aware of the possibilities of asynchronous attacks and seek adequate technical assistance if there are suspicious circumstances resulting from the activities of highly sophisticated and trained technologists. Evidence of such attacks would be discernible only from unexplainable deviations from application and system specifications in computer output or characteristics of system performance. Table 10 lists the potential perpetrators and methods of detecting asynchronous attacks.

Table 10

DETECTION OF ASYNCHRONOUS ATTACKS

Potential Perpetrators	Method of Detection	Evidence
Sophisticated advanced system programmers	System testing of suspected attack methods	Output that deviates from normally expected output or logs containing characteristics of computer operation
Sophisticated & advanced computer operators	Repeat execution of a job under normal and safe circumstances	

8. Scavenging

Scavenging is a method of obtaining information that may be left in or around a computer system after the execution of a job. Simple physical scavenging could be the searching of trash barrels for copies of discarded computer listings or carbon paper from multiple-part forms. More technical and sophisticated methods of scavenging can be done by searching for residual data left in a computer after job execution.

For example, a computer operating system may not properly erase buffer storage areas used for the temporary storage of input or output data. Some operating systems do not erase magnetic disk or magnetic tape storage media because of the excessive computer time required to do this. Therefore, new data are written over the old data. It may be possible for the next job to be executed to read the old data before they are replaced by new data. This might happen in the following way. If storage was reserved and used by a previous job and then assigned to the next job, the next job would gain access to the same storage, write only a small amount of data into that storage, but then read the entire storage area back out for its own purposes, thus capturing--scavenging--data that were stored by the previous job.

In one case, a time-sharing service in Texas had a number of oil companies as customers. The computer operator noticed that every time one particular customer used computer services his job always requested that a scratch tape (temporary storage tape) be mounted on a tape drive. When the operator mounted the tape, he noticed that the read-tape light always came on before the write-tape light came on, indicating that the user was reading data from a temporary storage tape before he had written anything on it. After numerous incidents of this, the computer operator became curious and reported it to management. Simple investigation revealed that the customer was engaged in industrial espionage, obtaining seismic data stored by various oil companies on the temporary tapes and selling this highly proprietary, valuable data to other oil companies.

The detection of scavenging usually occurs as a result of discovering suspected crimes involving proprietary information that may have come from a computer system and computer media. The information may be traced back to its source that involves computer usage. It is probably more likely that the act was a manual scavenging of information in human-readable form or the theft of magnetic tapes or disks rather than electronic scavenging.

In one case, valuable data were found on continuous forms from a computer output printer. [15]Each page of the output had a preprinted sequence number and the name of the paper company. An FBI agent was able to trace the paper back to the paper company. On the basis of the type of forms and sequence numbers, he traced it from there to the computer center where the paper had been used. The sequence numbers were traceable to a specific printer and time at which the forms were

printed. Discovery of the job that produced the reports at that time and the programmer who submitted the job from the computer console log and usage accounting data was straightforward. Table 11 lists the potential perpetrators. The table also summarizes the methods of detecting and the kinds of evidence typical with scavenging techniques.

Table 11

DETECTION OF SCAVENGING CRIMES

Potential Perpetrators	Method of Detection	Evidence
Users of the computer system	Tracing of discovered proprietary information back to its source	Computer output media
Persons having access to computer facilities and adjacent areas	Testing of an operating system to discover residual data after execution of a job	Type font characteristics
		Similar information produced in suspected ways in the same form

9. Data Leakage

A wide range of computer-related crime involves the removal of data or copies of data from a computer system or computer facility. [16] This possibility can offer the most dangerous exposure to the perpetrator. His technical act may be well hidden in the computer; however, to convert it to economic gain, he must get the data from the computer system. Output is subject to examination by computer operators and other data processing personnel.

Several techniques can be used to leak data from a computer system. The perpetrator may be able to hide the sensitive data in otherwise innocuous looking output reports. This could be done by adding to blocks of data. In more sophisticated ways the data could be interspersed with otherwise innocuous data. An even more sophisticated method might be to encode data to look like something different than they are. For example, a computer listing may be formatted so that the secret data are in the form of different lengths of printer lines, number of words or numbers per line, locations of punctuation, and use of code words that can be interspersed and converted into meaningful data. Another method is by controlling and observing the movement of equipment parts, such as the reading and writing of a magnetic tape causing the tape reels to move clockwise and counterclockwise in a pattern representing binary digits 0 and 1. Observation of the movement of the tape reels results in obtaining the data. Similar kinds of output might be accomplished by causing a printer to print and skip lines in a pattern where the noise of the printer, recorded with a

cassette tape recorder, might be played back at slow speed to again produce a pattern translatable into binary information.

These are rather exotic methods of data leakage that might be necessary only in high-security, high-risk environments. Otherwise, much simpler manual methods might be used. It has been reported that hidden in the central processors of many computers used in the Vietnam War were miniature radio transmitters capable of broadcasting the contents of the computers to a remote receiver. These were discovered when the computers were returned to the United States from Vietnam.

Investigation of data leakage would probably best be conducted by interrogatng data processing personnel who might have observed the movement of sensitive data. It might also be possible to examine computer operating system usage journals to determine if and when data files may have been accessed. Data leakage might be conducted through the use of Trojan horse, logic bomb, and scavenging methods. Possible use of these methods should be investigated when data leakage is suspected. Evidence will most likely be in the same form as evidence of scavenging activities described above. Table 12 summarizes the detection of crimes resulting from data leakage.

Table 12

DETECTION OF CRIMES FROM DATA LEAKAGE

Potential Perpetrators	Methods of Detection	Evidence
Computer programmers	Discovery of stolen information	Computer storage media
Employees Former employees Contract workers Vendor's employees	Tracing computer storage media back to the computer facility	Computer output forms
		Type font
		Trojan horse or scavenging evidence

10. Piggybacking and Impersonation

Piggybacking and impersonation can be done physically or electronically. Physical piggybacking is a method for gaining access to controlled access areas when control is accomplished by electronically or mechanically locked doors. Typically an individual usually with his hands full of computer-related objects such as tape reels stands by the locked door. When an authorized individual arrives and opens the door, the piggybacker goes in after or along with him. Turnstyles, mantraps, or a stationed guard are the usual methods of preventing this type of

unauthorized access. The turnstyle allows passage of only one individual with a metal key, an electronic or magnetic card key, or combination lock activation. A mantrap is a double-doored closet through which only one person can move with one key action. Success of this method of piggybacking is dependent upon the quality of the access control mechanism and the alertness of authorized persons in resisting cooperation with the perpetrator.

Electronic piggybacking can take place in an on-line computer system where individuals are using terminals, and identification is verified automatically by the computer system. When a terminal has been activated, the computer authorizes access, usually on the basis of a key, secret password, or other passing of required information (protocol). Compromise of the computer can take place when a hidden computer terminal is connected to the same line through the telephone switching equipment and used when the legitimate user is not using his terminal. The computer will not be able to differentiate or recognize the two terminals, but senses only one terminal and one authorized user. Piggybacking can also be accomplished when the user signs off improperly, leaving the terminal in an active state or leaving the computer in a state where it assumes the user is still active.

Impersonation is the process of one person assuming the identity of another. Physical access to computers or computer terminals and electronic access through terminals to a computer require positive identification of an authorized user. The verification of identification is based on some combination of something the user knows, such as a secret password; something the user is--i.e., a physiological characteristic, such as finger print, hand geometry, or voice; and something the user possesses, such as a magnetic stripe card or metal key. Anybody with the correct combination of identification characteristics can impersonate another individual.

An example of a clever impersonation occurred when a young man posed as a magazine writer and called upon a telephone company, indicating that he was writing an article on the computer system in use by the telephone company. [15] He was invited in and given a full and detailed briefing on all of the computer facilities and application systems. As a result of this information, he was able to steal over $1 million worth of telephone equipment from the company. In another case, an individual stole magnetic stripe credit cards that required secret personal identification numbers (PINS) associated with each card for use. He would call the owners of the cards by telephone indicting that he was a bank official, had discovered the theft of the card, and needed to know the secret PIN number to protect the victim and issue a new card. Victims invariably gave out their secret PINs and the impersonator then used the PINs to withdraw the maximum amount allowed through automatic teller machines that required the cards and numbers for identification.

Electronic door access control systems frequently are run by a minicomputer that produces a log showing accesses and time of accesses for each individual gaining access. Human guards frequently do equivalent journaling through the keeping of logs. Detection of unauthorized access can be accomplished by studying journals and logs and by interviewing people who may have witnessed the unauthoried access. Table 13 summarizes the methods of detecting computer crime committed by impersonation methods.

Table 13

DETECTION OF IMPERSONATION ACTS

Potential Perpetrators	Methods of Detection	Evidence
Employees, former employees, vendors' employees	Access observations	Logs, journals, equipment usage meters
	Interviewing witnesses	
Contracted persons	Examination of journals and logs	Other physical evidence
Outsiders	Specialized computer programs that analyze characteristics of on-line computer user accesses	

11. Wire Tapping

There is no verified experience of data communications wire tapping. The potential for wire tapping grows rapidly, however, as more computers are connected to communication facilities and increasing amounts of electronically stored assets are transported from computer to computer over communication circuits. Wire tapping has not become popular as far as is known because of the many easier ways to obtain or modify data.

Wire tapping requires equipment worth at least $200 (available at a Radio Shack store) and a method of recording and printing the information. Recording and printing can usually be done more directly and easily through the computer system or by impersonation through terminals. The perpetrator usually will not know when the particular data he is interested in will be sent. Therefore, he must collect relatively large amounts of data and search for the specific items of interest. Identification and isolation of the communications circuit can also pose a problem for the perpetrator. Interception of microwave and satellite communications represents even greater difficulty because

of the complexity and cost of the equipment to perform the operation. In addition, the perpetrator must determine whether there are active detection facilities built into the communication system.

The best method of protecting data is encryption or secret coding of the data using an encryption key. New, powerful products are now on the market to provide encryption. [17] It is anticipated that most valuable data will be routinely encrypted within the next several years. This probably will greatly reduce the threat of wire tapping.

Wire tapping should be assumed to be the least likely method used in the theft or modification of data. Detection methods and possible evidence will be the same as in the investigation of voice communication wire tapping. Table 14 summarizes the potential perpetrators, detection and evidence in wire-tapping acts.

Table 14

DETECTION OF WIRE TAPPING

Potential Perpetrators	Methods of Detection	Evidence
Communications technicians and engineers	Voice wiretapping methods	Voice wire tapping evidence
Communications employees		

12. Simulation and Modeling

A computer can be used as a tool or instrument of a crime for planning or control. Complex white-collar crime often requires the use of a computer because of its sophisticated capabilities. An existing process can be simulated on a computer or a planned method for carrying out a crime could be modeled to determine its possible success.

In one case involving a million dollar manual embezzlement, an accountant owned his own service bureau and simulated his company's accounting and general ledger system on his computer. [15] He was able to input correct data and modified data to determine the effects of the embezzlement on the general ledger. He also had the capability to run the simulation in the reverse direction by inputting to the computer the general ledger data he wished to have. He then ran the system in reverse to determine the false entries in accounts payable and accounts receivable that would result in the required general ledger output.

In one phase of an insurance fraud in Los Angeles in 1973, a computer was used to model the company and determine the effects of the sale of large numbers of insurance policies. [15] The modeling resulted in the creation of 64,000 fake insurance policies in computer-readable form that were then introduced into the real system and subsequently resold as valid policies to reinsuring companies.

The use of a computer for simulation and modeling normally requires extensive amounts of computer time and computer program development. Investigation should include a search for significant amounts of computer services used by the suspects in complex fraud. This can be done by determining recent business activities of suspects and investigating the customer lists of locally available commercial time-sharing and service bureau companies. If use of the victim's computer is suspected, usage logs may show unexplained amounts of computer time used by the suspects.

Usually a programmer with expertise in simulation and modeling would be required to develop the application needed. In some cases, it was found that the computer programmers had no knowledge that their work was being used for fraudulent purposes. Evidence in the form of computer programs, input data, and output reports would require the attention of a computer programmer expert or systems analyst to determine the nature of the modeling or simulation. Table 15 lists the potential perpetrators, methods of detection, and kinds of evidence in simulation and modeling techniques.

Table 15

DETECTION OF SIMULATION AND MODELING TECHNIQUES

Potential Perpetrators	Methods of Detection	Evidence
Computer application programmers	Investigation of possible computer usage by suspects	Computer programs Computer program documentation
Simulation and modeling experts		Computer input
Managers in positions to engage in large, complex embezzlement		Computer produced reports
		Computer usage logs and journals

SECTION II EXPERTS, WITNESSES, AND SUSPECTS

Computer-related crimes deal with people to a far greater degree than they deal with technology. Only people, and not computers, perpetrate, witness, or are the ultimate victims of these crimes. Therefore, investigators and prosecutors need to know more about the people and their functions in electronic data processing (EDP) than about the computer technology. Technical assistance can be obtained from experts.

This section is in two parts. The first part discusses who can provide technical assistance and the roles of each expert in using computers. In particular, the usefulness of computer security specialists and EDP auditors is emphasized. This will assist in orienting an investigator to the types of people he will encounter. Detailed descriptions of 18 occupations, including the skills, knowledge, computer access, and potential crime threats are provided in Appendix D.

The second part of this section discusses computer crime suspects. The vulnerabilities of computer systems to crime by people in specific occupations are emphasized. Characteristics of known computer criminals and aids for interviewing suspects are included.

A. TECHNICAL ASSISTANCE

It is particularly important that computer experts be used in computer-related crime investigation and prosecution. This applies to any technical field, not just computing. The best sources for obtaining experts are the victim's technical staff, the computer manufacturer of the equipment involved, other organizations that use identical computer equipment and similar software, local universities, computer technology consulting services, and service bureaus having similar equipment. Because of the close relationships among technologists, it is important to avoid the selection of an expert who may be an associate in some way with the suspects or may even be a suspect himself. The expert must be warned to keep his assistance a secret, especially among those people he knows and associates with on a professional basis.

When talking with computer people, a DDA should be prepared to interrupt for an explanation of every strange word used. It is important to understand each item before going on to the next. A glossary of terms as provided in this manual is most useful in this regard; however, it should be remembered that no consensus exists on the meanings of a number of technical terms in the computer field. Despite the precise nature of the technology computer experts are often not concerned with the preciseness of the technical terms they are using.

Investigators and prosecutors will usually encounter a wide range of distinct types of people and organizations in investigating computer-related crimes. Information about these types will enable the investigator to better evaluate their contributions during investigation, case development, and prosecution. Therefore, the subsections below provide distinctions among computer technologists who specialize in electronics, programming, and operations and also among data providers, users, systems analysts, and programmers who specialize in scientific/engineering information and business applications. Organizations range among those that use computers to conduct their business or services; those that manufacture computers, computer programs, and supplies; and those that provide computer services as a business. In addition, descriptions of computer security specialists and auditors who can be of great assistance are provided.

1. Electronics and Programming Experts and Witnesses

Computer technologists are frequently skilled in electronic circuitry in computers, but they know little about developing a significant computer program. Others are expert programmers but know little about the electronic aspects of the computers they use. This frequently is the case among computer maintenance engineers with electronic capabilities and application programmers with the latter capabilities.

An investigator should be aware of these differences in selection of experts and witnesses to supply information. Prosecutors experienced in questioning technologists strongly advise from the outset of an interview to insist on understanding all concepts and terminology as the interview progresses. The first questions should always determine the area of competence:

(1) What college degree do you have and what are the most recent courses you have taken?

(2) What is your current job title and job responsibility?

(3) What is the largest computer program you have written and when?

(4) What electronic components have you tested and when?

(5) Do you have sufficient experience and knowledge to answer the questions to be asked concerning _____?

It is also necessary to determine the knowledge and experience of an individual concerning the particular equipment or programming language of concern. A technologist, electronic or programming, will frequently be familiar with one manufacturer's equipment or programming

conventions but totally unable to answer questions about products of another company. Employment advertisements for programmers frequently specify the type and manufacturer of equipment or programming language to be used. In fact, a programmer may be an expert in COBOL programming but totally unknowledgeable in FORTRAN or BASIC (Beginners All-purpose Symbolic Instruction Code). Furthermore, if detailed technical questions are to be asked, a programmer experienced with one version of COBOL (COmmon Business-Oriented Language) may not be qualified in another COBOL despite the claim that both adhere to American National Standard Institute (ANSI) standard COBOL. [18]

It is advisable to assume that a computer technologist will be sufficiently knowledgeable about the details of a particular computer system or programming language only if he has recent, significant, and direct experience with it. Some computer facilities have one-of-a-kind computer operating systems, computer system configuration, or programming language for which only a few, specialized technologists may be qualified to answer questions. In some cases, application programs are still being used that were developed years ago on older generations of computers and that nobody is acquainted with in sufficient detail to answer detailed questions. Only the vendor's staff may sufficiently understand application programs and computers that run them that are purchased or leased for use.

2. Systems Analysts

One type of specialist, the systems analyst who may either not be in computer service departments or only indirectly associated with computers, is important in computer-related crime investigation and prosecution. Systems analysts engage in system requirements, specifications, and design activities and fall short of being computer users on one hand and programmers on the other. They tend to be specialized in certain applications and have backgrounds in either engineering disciplines or business functions but usually not both. They may have programming experience but are considered to be generally more senior than programmers. Some organizations have technologists called programmer analysts who tend to be more senior programmers usually specializing in applications and performing systems analysis as well as program design and development. Systems analysts may be valuable sources of information for investigators primarily because analysts usually are independent from yet thoroughly understand the function and activities of both the users and programmers.

3. Computer Scientists

More highly trained computer technologists are likely to be proficient in both electronics and programming. They usually have advanced degrees in computer science. These people also tend to be scientific-, mathematical-, or engineering-oriented rather than business-application oriented. Prosecutors should be aware that high degrees of specialization tend to limit computer scientists' knowledge of production business systems.

4. Computer Operators

Computer operations staffs normally consist of high school graduates with some trade school training. They frequently aspire to become programmers, and some may be part-time college students. Except for those learning to become programmers, their knowledge and skills are limited to operating equipment and following directions issued by the computer operating system and operations manuals. Computer operators usually have a good idea of the external characteristics of production jobs regarding run time, frequency of errors, and use of computer media such as tapes, disks, and paper forms. They will also be familiar with computer system performance reports, journals, exception reports, accounting data, and console logs.

5. Data Providers

Data providers can be divided into two general classifications: those in business systems and those in engineering and scientific programs. Business systems data providers are usually high school graduates--clerical people with relatively small amounts of training. Engineering and scientific data providers tend to have more training in engineering and scientific subjects. They often are college students or people with bachelor's degrees. These people usually know considerably more about the computer applications for which they are supplying data.

Large numbers of clerical people work to produce data processed in computer systems. Tellers in banks record their transactions through banking teller terminals that are connected directly to computers. They also fill out numerous forms that are keyed on to computer media by other clerks for computor processing. Others in banking run check sorters that automatically read magnetic ink character recognition MICR characters from the checks, and clerks key-in the check amounts for input to computers. Accounting clerks receive invoices and bills of lading that are checked, processed, and keyed into computers. Engineering aids collect data on construction and development projects covering many types of engineering. These data are keyed into computers for project development control and mathematical computations. Many workers are required to fill out their time cards or stamp their cards at time clocks. The hours-worked data are keyed into a computer system for timekeeping and payroll applications. The sources of data are endless.

These people usually are unacquainted with computer technology and never get near a computer. Yet the results of their work starts the whole process of computer production runs. Usually processes unknown to these people result in computer output reports that are often returned to many of the data providers to direct them in their work, thus closing the processing loop. There is little guidance possible for the investigator or prosecutor dealing with these people because they are so diverse and their jobs so different, depending upon the applications.

In some cases, these people view computer technology as a threat to their jobs as their functions become increasingly automated. Others see computer technology as a great aid in freeing them from tedious work.

Data providers are sometimes in a position to learn from experience the vulnerabilities of the computer systems they feed. They could engage in numerous kinds of fraud referred to as data diddling (See Section I) where they feed false data into the computer for their own advantage. These people are probably in the best position to convert their fraudulent acts directly into economic gain because they directly handle assets. They also frequently are unaware of the details of the computer production programs and of all the controls that may be built into these programs. A well-defined business data processing system would have extensive controls to detect deviations from normal activities that might be indicative of data entry fraud. Unfortunately, most business systems fall short of having effective detection controls. It is anticipated that as business systems are further developed and matured the data diddling or source entry fraud will be significantly reduced.

6. Computer Users

Computer users are managers and professional staff who are responsible for accomplishing tasks for which computers are used. These people may not understand computer technology, but they work with systems analysts and programmers who translate the users' needs into computer production systems.

Two distinct types of users, and the analysts and programmers who support them, are either business- or engineering-/scientific-oriented. Business users are usually people with middle to higher level business responsibilities. Included in this category of users are payroll, accounts receivable, and accounts payable managers; accountants; economists; and auditors. Business users tend to require large ongoing computer production systems that require periodic production runs, updating of large files of data and storage of data for future production. Such systems are usually I/O bound; i.e., the time required for computer processing is mostly the time for inputting data and producing reports.

The engineering/scientific users, systems analysts, and programmers tend to be people with engineering and scientific degrees who have significant knowledge of the particular subjects in which they are developing systems. These users include chemical, construction, mechanical and electrical engineers and biologists, physicists, chemists, and medical doctors in the practice of their professions. Engineering/scientic users tend to require computer programs that are run to solve specific problems but that are no longer needed unless similar problems arise for solution again. These computer programs tend to be computation bound, i.e., the production time is dependent on the computations performed by the computer and not the time for input and

output. Exceptions to this situation are sometimes found. Some engineering/scientific problems require massive amounts of input data, huge input-output bound computer production runs, and large amounts of output reports. However, these large production systems often tend to have shorter life than that of business systems because the solutions to problems are found or they are replaced with new and improved computer production systems.

With the increasing availability of inexpensive but powerful small computers, business and professional people are directly using them for small applications in both business and technical areas.

7. Information Systems Users and Developers

As the cost of storing large amounts of data in easily accessible computer media decreases, increasing numbers of information storage and retrieval systems are being developed. Examples are: library index systems; law retrieval systems such as Lexis and Westlaw; and parts inventory in large warehousing applications. The users are the receivers of the information storage and retrieval services. Systems analysts and computer programmers who develop these services specialize in data base management systems (DBMS).

A new occupation has developed called data base manager. This individual is responsible for the overall administration of large files or data bases of information. His job is to ensure the effective use, expansion, and integrity of large data bases.

Increasing interest in management information systems (MIS) has resulted in new specialties among users, system analysts, and programmers. A MIS is a storage and retrieval data base application that provides key information to aid managers in their work. A MIS usually consists of files of different kinds of information and a set of applications that processes and analyzes information usually of an operational nature; it reduces the information to detail and summary reports that are made available to the organization's management hierarchy.

Crimes associated with DBMS and MIS applications tend to be sabotage, espionage, and highly sophisticated frauds involving information more than money. Technology associated with large DBMS and MIS applications is highly complex. Investigators and prosecutors are well advised to seek expert advice if it is necessary to deal with this technology.

8. Computer-Related Organizations

It is often important for the investigator and prosecutor to know and understand the politics and current state of an organization

relative to its use of computers. This is particularly true in business fraud, where an organization or a major part of it may be engaged in fraudulent activities.

It is important that investigators and prosecutors understand and anticipate the different kinds of organizations with which they may interact in both investigating and prosecuting a computer-related crime. Organizations are identified in the following three major categories:

- o Those that use computers to conduct their business or services.
- o Those that manufacture computers, peripheral equipment, computer programs, and computer-related supplies.
- o Those that provide computer services as a business.

Each of these categories is discussed below.

a. Computer User Organizations

Top management among organizations that use computers consider computers as a necessary service function within their organizations. Top management frequently does not understand the technology, and data processing managers have significant power within organizations. These organizations either have and operate their own computers, have their own computers and contract to a facilities management company to operate for them, or do not have computers but use outside computer service companies to do their processing. Many organizations also engage in various combinations of these methods of using computers.

It can be important for an investigator to understand where the use of computers fits managerially into the organizations. Some large organizations that use computers for applications beyond the running of the business, such as for engineering, research, etc., will frequently have two kinds of computer centers: one for business data processing and one for engineering and scientific data processing. These are rarely combined in a single computer system because of the differences between the requirements for personnel needed to operate and program them. Where they are combined in one computer center, a degree of conflict often occurs between these two different groups of people.

The proliferation of low-cost minicomputers and time-sharing services has moved computing activity into the specific departments that need computer services. A large business or government organization may have one or more large central computer centers, ten or even 100 minicomputers in individual departments, and several hundred people using outside commercial time-sharing services through computer terminals and telephone circuits. Debate in the computer field continues over the advantages and disadvantages of large centralized computer facilities serving an entire organization versus various configurations of distributed computing. One of the world's largest

banks has recently gone through a massive distribution of small computers out to the individual departments that need computer services. It has replaced the large central computer facilities with hundreds of minicomputers.

On the other hand, other large businesses are in the process of centralizing what was once a widely distributed array of computers. Computer technology now supports both of these types of configurations on an economic basis. Therefore, the decisions in making a choice tend to be based on the type of organization and the specific kinds of computing needs of each suborganization.

b. Manufacturing Organizations

Organizations that manufacture computers, peripheral equipment, computer programs and supplies may be sources of information for the prosecutor or investigator. Conversely, he may be investigating an alleged crime within one of these organizations. Because these organizations tend to be large, complex businesses, they are frequently users of their own products; hence, they are the same in this respect as the organizations discussed above. In obtaining information from manufacturing organizations, it is important to find individuals with sufficient expertise to provide adequate information. It may be effective to start the search for the qualified individuals by contacting the public relations office or internal audit department in that these two departments tend to have a breadth of knowledge about the organization. Many businesses will be eager to provide significant amounts of information free of charge as a public duty or out of self-interest to minimize the negative image of their products that result from a company's involvement in a computer-related crime.

c. Computer Service Organizations

Organizations that provide computer services as their business tend to be highly technically oriented. The two basic kinds of services offered are: service bureau batch services and time-sharing services. Most large service companies now offer both of these types of services. However, hundreds of small service bureaus still pick up input from their customers, perform the computer processing, and return the output to them.

These companies tend to be highly competitive. Consequently, several cases of industrial espionage and sabotage have occurred among them. Employees of computer services organizations tend to be in high positions of trust because they have wide access to the often sensitive data of their customers. Therefore, computer service organizations tend to have more advanced security than other organizations and often emphasize security in their advertising. The investigator will usually find that these organizations are highly reluctant to supply information about the nature of their customer's data processing. Like banks, they try to protect their security and safety image.

These organizations sometimes specialize in certain types of data processing. Some may sell their services to provide business data processing, some may concentrate on engineering/scientific data processing, and others may offer specialized information services. These organizations also provide various amounts of systems analysis and computer programming services. An organization may provide complete services in the design, development, and production of application systems. Others may provide only the computer services, leaving it up to their customers to develop their own computer programs.

Computer service organizations are now offering more common computer applications. If a user can fit his application's needs into a preprogrammed package, he can significantly reduce the costs of computer program development. The competitive nature of these organizations is currently resulting in each organization trying to provide a wider range of more sophisticated application programs than those of its competitors. The application programs are normally available only for use with their computer systems and are not sold or licensed directly to the users. These programs tend to be protected as trade secrets rather than copyrighted.

9. Personal Computer Users

A new range of products and markets has recently developed around the microcomputer. Microcomputers are small, breadbox-size computers that are as powerful as computers that occupied entire rooms a few years ago. The market for these microcomputers is large, and numerous retail stores have been specializing in them. Tens of thousands of personal computers are expected to be in the hands of individuals in their homes, offices, and schools in the next several years. They will also be interfaced to resident telephones with as yet unknown consequences.

This puts a new powerful tool into the hands of criminals. A telephone company in Pennsylvania was recently attacked by Cap'n Crunch (John Draper) using a personal computer in an automated phone-freaking, blue-box type of criminal activity. In another case, a small computer was used to automate one of the largest, most complex, check kiting schemes in which the computer was used to keep track of all accounts, account balances, and check passing.

Microcomputers are also becoming popular in small business and professional offices where they can perform the same functions that computers perform in larger organizations. An offshoot of this microcomputer technology is word processing for which microcomputers form the basis for the typing, editing, and production of text including letters, manuals, reports, and books.

Applications programs for personal computers are frequently sold through computer retail stores. A small magnetic disk containing the program and a manual describing its use often will be packaged together. These programs are normally licensed and many, although not all, are

protected by copyright. Program piracy now exists and may be on the increase. Program owners, who are often small businessmen without the financial capacity to undertake the expense of a civil suit for copyright infringement or unfair competition, have already taken complaints to federal and state prosecutors for action pursuant to criminal law.

If a microcomputer is involved in an alleged crime, the investigator or prosecutor could seek technical advice from any of the many retail stores that sell this equipment. It is important, however, to seek advice from an individual who is familiar with the particular type of microcomputer because of the high degree of specialization in this field.

10. Computer Security Specialists

Computer-related crime acts include the violation, neutralization, or avoidance of safeguards and controls that would otherwise prevent or detect the illegal act in a timely way. Therefore, it is important to be aware of the role of the computer security specialist who assists in the protection of organizations using computers.

Computer security is in a state of early development. A number of universities, research institutes, computer manufacturers, and government agencies are making efforts to apply analytical methods to computer security and develop the needed safeguards and controls. Improvements are being made to keep pace with the increasing amounts of assets that are being stored and processed in computers and transferred over telephone circuits. (See Section III.B.2. for a discussion of security in a data center.)

Prosecutors and investigators should be aware that the people responsible for the advancement of computer security are primarily computer technologists who lack industrial security or criminal justice backgrounds. They generally tend to treat computer security as a technical subject that is amenable mainly to technical solutions. They often fail to understand that computer security is primarily a problem with the behavior and activities of people and that there is a real enemy intent on harming the assets and possibly people in an organization. At the same time, specialists in industrial security and people with criminal justice backgrounds have not gained sufficient technical capabilities to effectively apply their knowledge and backgrounds to computer security problems.

Computer security is the generic term used here to identify all kinds of safeguarding and controls to ensure the safe use of computer technology. Data security is another generic term often used to cover this whole subject. However, data security is meant to be security directly associated with the protection of data and does not include the protection of computer personnel, facilities, equipment, and computer programs. [19] It is important for investigators and prosecutors to

understand computer security and the role of the security specialist because computer-related crime invariably involves the compromise of security.

a. Responsibility for Security

The responsibilities for security in a large data processing department are usually split among employees, managers, computer security specialists, computer auditors, and staff functions in the business, such as the industrial security or protection department, the insurance department, personnel department, and other such functions. Security is the direct responsibilty of each manager in his particular area of management activity. The auditors act in a staff capacity assisting line management by determining the effectiveness of the security in a line manager's area. The computer security specialist or computer security coordinator also has the responsibility of assisting line managers. The security specialist usually has specific security responsibilities for administration of passwords for access to the computer and physical access controls in the use of badges and keys. He is also responsible for producing the overall plans for security and the procedures for implementing them. Each employee has a security responsibility to his employer to assure that his work is conducted in an appropriate, secure manner.

b. Security Organization

Computer security in most organizations is planned, developed, and implemented within the computer services area of an organization rather than in the traditional area of the industrial security or protection department concerned with physical security throughout the entire organization. The reason for this segmentation is that industrial security specialists have not yet gained sufficient capabilities in computer technology to deal with the complexity and differences in computer security. Focusing computer security in the computer services department often results in suboptimization of security because the function does not have sufficient authorization to impose security among the users of the computer services in other parts of the organization. Internal audit departments are frequently given the assignment of evaluating the degree of security and identifying the vulnerabilities across the organization wherever computer services are offered and used (See Section II.A.11.c.).

The computer security specialist is a new occupation formed within the last 3 or 4 years. It is not yet a well-formed occupation. Requirements and experience have not been generally agreed upon, and there is no course of study that prepares an individual for this occupation. Computer security specialists generally come from technical jobs, such as computer programming, systems analysis, or computer operations management within the computer field. Only the very largest computer organizations have established one or more full-time computer security specialists or coordinators. More often, an individual in

lower management or a technologist from a standards, procedures, and training function is appointed to coordinate computer security on a part-time basis as only one of his responsibilities. Other organizations from time-to-time establish temporary task forces or committees to perform security evaluations and make recommendations to management.

11. Auditors

Auditors are particularly helpful in economic crime investigation and prosecution. The specialization of some auditors in computer technology make this expertise also of value in computer-related crime work.

The EDP auditor can be an excellent source of information and assistance in an investigation. Because the function is based on (or may actually be a part of) internal audit, important professional standards and principles dictate how work is performed. This gives strength and credence to EDP audit as a reliable source. Specific information on controls, weakness in security, recommendations for strengthening controls, and general information on elements of the EDP environment should be readily available. Also, the EDP auditor often has computer tools specifically designed to assist in reviewing, testing, and evaluating computerized records and computer systems. (Appendix E describes a number of the most relevant EDP audit tools.) Initially learning to use an audit tool can be very time consuming, and any possible assistance from EDP auditors should be taken. Some EDP auditors may be chartered and experienced in the investigation of computer-related fraud or abuse. This is more a function of the policy of the company and the specific auditor than a general attribute of the position.

The following items are the major strong points of EDP audit in terms of typical assistance in a computer-related investigation:

- Level of confidence. Because of the nature of the audit profession, auditors are highly respected as analysts and evaluators; there are well-established standards, principles, and codes of ethics that dictate how auditors will conduct their work; to a degree, an auditor has responsibility to his profession as well as his company.

- Technical expertise. With proper training and experience, EDP auditors will provide a high level of EDP technical knowledge, both for the data processing profession in general and the specific computer environment within the company.

- Tools and techniques. Because EDP auditors must regularly use EDP audit tools and techniques, they are often available for testing and investigation; the EDP auditor should have some of

these ready for immediate use (especially a generalized audit computer program package that can be used for retrieving and analyzing computerized records).

- Independence. Because an auditor has no direct responsibility for nor authority over any of the activities that he reviews, he has a broad mandate, and he reports to a high level (e.g., the board of directors), his independence is well established; this factor is critical in any investigation.

The following items are the major weak points of EDP audit in terms of typical assistance in a computer-related investigation:

- Relationship in organization. Because audits are evaluations of the organization, they are often the cause of disagreement between EDP audit and the audited group; this can result in an adversary relationship that may compromise cooperation.

- Inexperience of profession. Because of the relative newness of EDP and the EDP audit profession in contrast to the general field of audit, there is a lack of "generally accepted" EDP audit principles, standards, guidelines, and tools and techniques; there is a wide variance as to what individual corporations are doing in the field.

- Training. The lack of standard training or formal education programs results in wide variance in the level of EDP auditor expertise; some have excellent EDP and audit backgrounds, others are much stronger in one area than the other, and some have entered the profession with a very low level of EDP audit knowledge.

a. Audit Organization

Most large organizations, both in the private and public sector, have internal audit departments. These departments provide an independent appraisal of operations as a service to senior management (independent from a department or functional viewpoint, but still part of the same corporation). They function as a managerial control by measuring and evaluating the effectiveness of other internal controls. Although there is no formal requirement to have an internal audit function, the Securities and Exchange Commission (SEC) strongly recommends that organizations falling under the SEC Act of 1934 have such a function.

Many of these organizations that have significant data processing equipment and computerized systems also have an EDP audit function. This function may be a separate department, part of internal audit, or part of some other department. The EDP audit function also serves as an independent tool for senior management to evaluate internal controls in and for the EDP environment.

The need for EDP auditing has come from a change in the way the computer stores and processes data rather than from a change in accounting theory or auditing principles. New tools, techniques, methods, and auditor expertise are required.

Another auditing group is the independent external auditors. They are totally independent from the corporation being audited and are paid to conduct the audits (at least yearly).

b. External Auditors

Independent public accounting firms audit corporations and certify the accuracy of corporate financial information (for example, the statement in a company's annual report). These audits are performed under the provisions of the federal securities laws. When acting as the independent auditor of a publicly owned corporation, the external auditor has public responsibilities and must satisfy requirements of the federal government regarding performance of those responsibilities. The objective of the ordinary examination of financial statements by the independent auditor is the expression of an opinion on the fairness with which they present financial position, results of operations, and changes in financial position in conformity with generally accepted accounting principles.

CPAs (certified public accountants), certified by state examining boards as having met stringent qualifying requirements to practice accounting, may serve as independent auditors for publicly owned corporations. Noncertified accountants may engage in some of the audit work, but a CPA is required to direct the effort and to sign the opinion.

The American Institute of Certified Public Accountants (AICPA) is the national association that guides and directs the auditing profession. Various committees of the AICPA are chartered to issue pronouncements and rules on auditing matters; for example, "Statement on Auditing Standards Number 3, The Effects of EDP on the Auditors' Study and Evaluation of Internal Control". [20] There is a code of professional ethics that supports the standards and provides a basis for their enforcement.

The major purpose of external auditing is to attest to the accuracy of financial statements of a company and not to audit internal controls per se (e.g., controls involved with data processing). However, a number of firms have developed audit tools to assist in EDP auditing. The major tool is called a Generalized Audit Computer Program Package and is used to retrieve and analyze data stored in computer files.

From an EDP perspective, external auditors typically do not get into a detailed review of the full computer environment--the financial attest does not require that type of effort. Nonetheless, they usually have staff with EDP expertise and use them as needed, typically for

either helping extract computerized financial records or for management consulting on special projects (other than the attest function).

External auditors normally produce two reports, the opinion letter and a management letter. The opinion letter is a short statement of the scope and date of the audit, an opinion of the accuracy and "fairness" of the financial statement, any exceptions, and whether the financial statements are presented in accordance with generally accepted accounting principles that have been consistently observed over the preceeding periods. The management letter includes findings regarding weak or missing controls and recommendations for corrective action. In addition to producing these formal reports, external auditors have well-defined standards of field work that include the compilation of sufficient evidential matter (in work papers) to support the rendered opinion.

The consideration for fraud responsibility is precisely defined in the AICPA's "Codification of Auditing Standards and Procedures." [21] The reference is not limited to any one area such as EDP but is an overall position:

> ...opinion on financial statements is not primarily or especially designed, and cannot be relied upon, to disclose defalcations and other similar irregularities, although their discovery may result....The responsibility of the independent auditor for failure to detect fraud (which responsibility differs as to clients and others) arises only when such failure clearly results from failure to comply with generally accepted auditing standards.... The subsequent discovery that fraud existed during the period covered by the independent auditor's examination does not of itself indicate negligence on his part. He is not an insurer or guarantor; if his examination was made with due professional skill and care in accordance with generally accepted auditing standards, he has fulfilled all of the obligations implicit in his undertaking.

c. Internal Auditors

Internal audit is the primary function for reviewing and evaluating controls within an organization. The mandate of the function normally includes the review of the entire scope of an organization, not just financial and accounting. Internal audit often is the only group concerned with the total organization, cutting across department boundaries. This is especially important in relationship to EDP because computerized application systems involve several departments almost by definition.

The objective of internal audit is to assist all members of management in the effective discharge of their responsibilities.

Internal auditors furnish management with analyses, appraisals, recommendations, and pertinent comments concerning the activities reviewed.

The scope of the internal audit mandate varies from organization to organization but is usually quite broad. The Institute of Internal Auditor's (IIA) "Standards for the Professional Practice of Internal Auditing" defines the scope of work as: "The scope of the internal audit should encompass the examination and evaluation of the adequacy and effectivenss of the organization's system of internal control and the quality of performance in carrying out assigned responsibilities." [22]

Certified Internal Auditors (CIAs) have been certified by the IIA. Certification includes subscribing to a code of ethics, holding a baccalaureate degree or equivalent work experience, and passing an examination based on a "Common Body of Knowledge for Internal Auditors." [23] The CIA rating was established to promote and increase the professional standing of internal auditors but is not a requirement for being an internal auditor.

Internal auditors normally produce audit reports for management that contain their findings regarding weak or missing controls and recommendations for corrective action. As with external auditors, there are well-defined standards of performance that include the compilation of information to support all audit work. These work papers can be very helpful in subsequent investigations of related matters.

The issues of detecting and investigating fraud and other irregularities have varied over the years and from one organization to another. Some organizations do not charter their internal audit function with responsibility for detecting fraud, justifying this on a cost benefit basis. Other organizations see the internal audit function as both detecting fraud and acting as a deterrent to fraud. The consideration for fraud detection is directly addressed in the IIA's "Standards for the Professional Practice of Internal Auditing." [22] The reference is not limited to any one area such as EDP, but is a general standard dealing with due professional care.

> ...in exercising due professional care, internal auditors should be alert to the possibility of intentional wrongdoing, errors and omissions, inefficiency, waste, ineffectiveness and conflicts of interest. They should also be alert to those conditions and activities where irregularities are most likely to occur. In addition, they should identify inadequate controls and recommend improvements to promote compliance with acceptable procedures and practices.
>
> Due care implies reasonable care and competence, not infallibility or extraordinary performance. Due care requires the auditor to conduct examinations and verifications to a

reasonable extent, but does not require detailed audits of all transactions. Accordingly, the internal auditor cannot give absolute assurance that noncompliance or irregularities do exist. Nevertheless, the possibility of material irregularities or noncompliance should be considered whenever the internal auditor undertakes an internal auditing assignment.

When an internal auditor suspects wrongdoing, the appropriate authorities within the organization should be informed. The internal auditor should recommend whatever investigation is considered necessary in the circumstances. Thereafter, the auditor should follow up to see that the internal auditing department's responsibilities have been met.

The Bank Administration Institute (BAI), also concerned with standards of internal auditing, has a statement on the internal auditors responsibility for detecting fraud. The statement appears in the BAI's "Statement of Principle and Standards for Internal Auditing in the Banking Industry." [24]

Audit proficiency includes the ability to evaluate fraud exposures. Sufficient information is available in the literature on auditing concerning how frauds may be committed in banking. The auditor should be familiar with that literature.

The systems of control and not the internal audit function provide the primary assurance against fraud. Internal auditors, however, must evaluate the capability of the systems to achieve that end. When in doubt the auditor should consider applying additional procedures to determine if fraud has actually occurred.

In fixing the internal auditor's responsibility for detecting fraud, it should be recognized that the internal auditor cannot be responsible for detecting irregular transactions for which there is no record, e.g., an unrecorded receipt of cash from a source for which there is no evidence of accountability; an isolated transaction that does not recur, e.g., a single fraudulent loan; or irregularities that are well concealed by collusion. However, in the usual course of the audit cycle, the internal auditor should detect irregularities that significantly affect the financial statements, repeatedly follow a suspicious pattern of occurrence, or those that can be detected by a reasonable audit sampling. Internal auditors must also accept responsibility for those irregularities that result from their failure to report known weaknesses in the systems of control.

In judging the preventive capacity of the control systems and the internal auditor's responsibility, the principle of relative risk should not be ignored, namely, costs must be balanced against intended benefit.

a. EDP Auditors

EDP auditors may be a part of internal audit or established as a separate group. The general charter for EDP audit is similar to that of internal audit. Many EDP auditors were originally internal auditors.

The scope of EDP audit is oriented to and centered in the data processing environment, but must extend to nonautomated areas that affect the computerized area. The major elements of data processing that are audited are: computer service centers--the hardware and facilities; computer application systems--the production programs; and application systems development--the process of designing, implementing, and changing the production programs.

The EDP audit profession and EDP audit departments are relatively new as compared with those of external auditing and general internal auditing. There is not an established set of principles, standards, and guidelines specifically oriented to EDP audit. As of 1979, the certification program is just being established. This certification program for EDP auditors, Certified Data Processing Auditors (CDPA), is administered by the EDP Auditors Foundation. [25] The program includes an examination and subscription to a code of ethics.

Internal audit staff size varies considerably depending on factors such as the size of the organization, type of industry (e.g. financial or regulated industries will have relatively more), degree of automation, and attitude of top management (apparently more important a factor for EDP audit than for internal audit staff size). In a research report by The Conference Board [26], 75% of the companies surveyed and 100% of the companies in the banking industry had EDP auditors.

The background of EDP auditors is often a mixture of auditing (internal and/or external) and data processing. Typically, because of the complexity of the EDP profession, it takes more time and effort to train an auditor in data processing than to train a data processor in auditing. However, there are important auditing concepts and perspectives that are products of experience and are often not adequately developed in training EDP auditors.

Topics or education courses that EDP auditors should have taken include:

- o Basic topics: introduction to DP, computer hardware overview, computer programming overview, computer documentation overview, introduction to DP application controls, and introduction to general DP controls.

- o Advanced topics: on-line systems controls, data communication controls, continuous operation controls, storage media/device controls, audit trace considerations, and special audit software.

A number of different tools and techniques are used by EDP auditors to audit the computer environment and may be of help in investigation and prosecution. The tools and techniques can be classified by the function that they perform.

- o Auditing systems development and change control: code comparison and system acceptance and control group.

- o Computer application control testing: test data method, base-case system evaluation, integrated test facility, and parallel simulation.

- o Selecting and monitoring transactions for compliance, testing, and data verification: transaction selection, embedded audit data collection, and extended records.

- o Data verification: generalized audit computer program.

- o Analysis of computer programs: snapshot, tracing, mapping, and control flowcharting.

- o Auditing computer service centers: job accounting data analysis.

The most widely used tool is the generalized audit computer program package. The other tools and techniques that have been used the most are: test data method, transaction selection, and control flowcharting. Brief descriptions of these 15 EDP audit tools and techniques and a list of computer-related occupations of possible suspects (from Appendix D) that could be affected by the use of the tools are given in Appendix E. [26].

B. SUSPECTS

This section provides aids for identifying and dealing with suspects. The populations of people that represent potential threats based on their skills, knowledge, and access to resources are identified

are ranked below in order of potential loss they could cause in an idealized, hypothetical computer center. The results would not necessarily be the same in any computer center because of differing practices and safeguards. In a computer enviroment, four basic sources of potential perpetrators can be established. These are:

- o People with physical access to assets and the capabilities to perform physical acts;
- o People with access and operational capabilities;
- o People with access and programming capabilities;
- o People with access and electronic engineering capabilities.

This suggests an approach to identifying these people by their skills, knowledge, and access in terms of occupations. The people to be considered may include not only employees, but also managers and any others who have sufficient skills, knowledge, and access to represent potential threats to computer resources.

Table 16 presents the results of a vulnerability analysis associated with five possible acts against eight forms of assets and general types of safeguards for each occupation. The ranges of exposed assets have been subjectively assigned to each occupation and occupations have been ranked in five levels according to degree of exposure.

The matrix entries in Table 16 are based on the following exposure scale of blank (no effect) and numbers 1 to 5 indicating the percentage of the asset that an individual could affect:

Scale	Percentage of Effect on Asset
Blank	No effect
1	To 20
2	To 40
3	To 60
4	To 80
5	To 100

An entry of 5 on the line of a particular occupation in the column "Internal Data/Disclosure" indicates that an individual is in a position to disclose almost all data internal to the system. An entry of 2 indicates the ability to affect up to 40% of the data in the same way. A blank entry denotes no effect.

Table 16
OCCUPATIONAL VULNERABILITY ANALYSIS

Acts

M--Modification
DE--Destruction
DI--Disclosure
T--Taking
DN--Denial of use

Exposure Scale

blank	no effect
1	up to 20%
2	up to 40%
3	up to 60%
4	up to 80%
5	up to 100%

Vulnerabilities: Physical, Operational, Programmable, Electronic

Page No.	Occupations	Internal Data M	Internal Data DE	Internal Data DI	Internal Application Programs M	Internal Application Programs DE	Internal Application Programs DI	Internal System Programs M	Internal System Programs DE	Internal System Programs DI	External Data M	External Data DE	External Data DI	External Application Programs M	External Application Programs DE	External Application Programs DI	External System Programs M	External System Programs DE	External System Programs DI	Computer Equipment & Supplies M	Computer Equipment & Supplies DE	Computer Equipment & Supplies T	System Service T	System Service DN
(16)	Tape librarian										4	4		3	3		3	3		1	1			
(17)	User tape librarian										2	2		1	1					1	1			
(8)	User trans. & data entry operator	2	2	2		1	1				2	2	2		1	1				1	1			
(10)	Computer operator	1	5	5		5	5		5	5	1	3	3							5	5		5	5
(12)	Peripheral equipment operator										3	3		4	4		1	1		2	2			
(13)	Job set-up Clerk										3	3		4	4					1	1		5	
(14)	Data entry & update clerk	3	3	3		4	4		5	5	3	3	3		4	4		1	5	1	1			
(29)	Facilities engineer																			1	5	5		5
(30)	Operations manager	1	5	5		5	5		5	5	1	3	3		4	4		1	5		5	5	5	5
(32)	Data base administrator	3	3	3							3	3	3								1	1		
(18)	System programmer		5	5		5	5	5	5	5							5	1	5		1	1	5	5
(20)	Applications programmer	1	1	1	2	2	2							2	2	2					1	1		
(22)	User programmer	1	1	1	2	2	2							2	2	2					1	1		
(33)	Programming manager	1	1	1	4	4	4							4	4	4					1	1		
(27)	Communication Engineer/Operator		5	5																2	2	2		
(24)	Terminal Engineer																			1	1	1		
(25)	Computer system engineer							2	2	2										5	5	5		
(35)	Security officer	5	5	5	5	5	5		5	5	5	3	3	3	4	4	4	5	5	5	5	5	5	5
(36)	EDP auditor	5	5	5	5	5	5		5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5

Assets in the form of data, application programs, and system programs are designated as internal to a computer system when the central processor has continuous access to them from any attached storage device. Assets are considered external to a computer system when they are in human-readable or computer-readable form and where computer personnel have manual, direct access to them. Computer equipment, supplies, and services complete the range of types of assets.

Three types of acts, and in one case, two, are stated for each form of asset. Modification (M) is the intentional addition, deletion, or replacement of the asset. Destruction (DE) is rendering the asset totally useless. Destroying part of a data record, but leaving an identifiable and usable part intact, is considered modification, not destruction. Disclosure (DI) is unauthorized revealing of data or programs by observation, taking, or using. Taking (T) is the unauthorized removal of computer supplies, equipment, or use of computer resources. Denial of use (DN) applies to services and resources. In all acts, it is assumed that a perpetrator does profit or could profit from his act and that a victim does experience or could experience a loss from the act.

The matrix entries in Table 16 reflect an environment in which usual safeguards and controls have been installed in idealized, totally effective ways. Different matrix entries might be assigned for a specific computer facility based on its actual environment and safeguards in place. For example, whenever it is possible to limit the access and functioning of an individual, the study assumes that this is done. One reason that the application programmer and the user programmer are assigned a limited exposure level rather than a great exposure level is that it is assumed that these individuals communicate with the system through a programmer terminal or intermediary. They never have access to current production, and independent computer program verification occurs before their products are put into production. Similarly, it is assumed that the computer system engineer is never permitted to work on a computer system when any production data or application programs are present.

Occasional ambiguity exists in the classification of a particular act. For example, a system programmer might modify a system program internal to the system and successfully deny authorized system service. In this situation, the convention adopted is to classify the violation in the category that had to occur first. Therefore, this example would be classified as an internal modification of a systems program rather than a denial of system service.

Note that occupations are described in generic and idealized form in terms of job function, skills, knowledge, and access. In practice, the skills, knowledge, and access of personnel do not match exactly these descriptions of their occupations. It is assumed here that each occupation is limited to only the description provided. For example, a computer operator who has programming skill, knowledge, and access in

addition to his operator capabilities must be classified as a programmer as well as a computer operator in the scheme of this report. If he functions in both capacities, then the two occupations presented here must be combined in depicting the individual as a source of exposure to loss, and all vulnerabilities and safeguards in both descriptions apply to the individual.

Collusion of two or more individuals is not considered. It is always assumed that each individual performs a single act alone with a single asset. In actual experience, a loss often results from sequences of parallel independent and dependent acts involving several assets in several forms. A listing of occupations by risk level appears in Table 17. Descriptions of 19 occupations are presented in Appendix D. Each description includes function, knowledge, access, vulnerabilities, risk level, general safeguards, and conclusions.

Table 17

RISK LEVEL OF OCCUPATIONS BASED ON RANGE OF ASSETS EXPOSURE
(Occupations in Alphabetical Order Within Risk Level)

Greatest risk
- EDP auditor
- Security officer

Great risk
- Computer operator
- Data entry and update clerk
- Operations manager
- Systems programmer

Moderate risk
- Computer system engineer
- Programming manager

Limited risk
- Application programmer
- Communication engineer/operator
- Data base administrator
- Facilities engineer
- Peripheral equipment operator
- Tape librarian
- User programmer
- User transaction and data entry operator

Low risk
- Terminal engineer
- User tape librarian

1. Suspects' Characteristics and Circumstances Based on Experience

Suspects may be identified on the basis of characteristics of known computer-related crime perpetrators who have been interviewed in computer abuse studies. [26] According to the results of interviews with this small group of 25 perpetrators, organizations will be more

vulnerable to people with the following characteristics and where these circumstances are present. Experienced investigators may find little difference between these characteristics and those of the modern-day, amateur, white-collar criminal. Moreover, these characteristics cannot be considered conclusive or complete because they are identified from such a small number of perpetrator interviews. Nevertheless, the documentation of them here should aid or recall for the investigator important clues to computer-related crime suspects.

a. Age

Anticipate that perpetrators tend to be young. The median age is 25 years and the range is 18-46 years. Younger people in data processing occupations tend to have received their education in colleges and universities where attacking campus computer systems is not only condoned but often encouraged as an educational activity. Younger people as compared with older employees, have often not yet been assimilated into the profession and may not have taken on the professional responsibilities and identity with the organization of their employer.

b. Skills and Knowledge

Anticipate that suspects will be among the most skilled and higher performing technologists. One of the greatest vulnerabilities in an organization comes from workers who are over qualified for the work that they are doing. An abundance of bright, highly motivated technologists enter the computer field and find themselves placed in routine jobs requiring low levels of skill--e.g., programmers engaged in the detailed work that leaves little room for innovation and recognition. These people become easily frustrated and look for other possibly illegal ways of using their skills, knowledge, and energy. It is important to note that 5 of the 17 perpetrators were high-experience professionals and 7 were managers.

c. Positions of Trust

In most cases, perpetrators performed their acts while engaged in their occupations in their work environments. One exception to this is an individual who, while president of an electronics supply house, posed as a telephone company employee to order the delivery of telephone equipment through the telephone company computer system. However, even in this case, the individual had to pose as an employee to obtain the necessary information to engage in his fraud. When investigating a potential loss, anticipate that the vulnerability will be identified and the person(s) most qualified will take advantage of it. The most likely suspects in any computer-related crime involving computer technology will be those, usually few, people who have the necessary skills, knowledge, and access. If a crime involves computer programs, anticipate suspects among the computer programmers who have access to and knowledge of the computer programs or through those programs to the

assets found to be missing. If the vulnerability discovered is in the data entry function, then anticipate that suspects may be among the data entry clerks. Next consider all other technical functions where vulnerabilities may arise. Computer programmers are not likely to go into the foreign environment of the data entry section to engage in unauthorized technical acts. Neither will data entry clerks attempt to modify or introduce computer programs into a computer to engage in criminal acts. They will most often limit their activities to their own work areas that they know the best, and usually they know that particular area better than anyone else in the world. Table 18 lists the occupations of perpetrators of computer-related crime and the types of victims.

Table 18

RELATIONSHIP OF PERPETRATOR OCCUPATIONS TO TYPE OF VICTIM

Perpetrators' Occupations	Victims
Teller	Large bank
Accountant	Computer service
Company owner	Small manufacturing company
Time-sharing user	Time-sharing computer system
Business programmer	Small bank
Systems programmer	State, government agency
Computer operations and systems manager	Financial institutions
President of a firm	Electronics supply company
Business manager	Large manufacturer
Sales manager	Large retail service organization

d. Assistance

Perpetrators have been found to need assistance in one-half of all known computer-related crimes, whereas ordinary white-collar crime, embezzlement for example, involved a low degree of collusion according to a study of 271 bank frauds and embezzlements. [27] Therefore, in the investigation of an alleged computer-related crime, it is best to assume that more than one perpetrator may have been involved. The reason for high collusion is probably because it takes more skills, knowledge and access than one individual possesses to complete a computer-related crime. Collusion usually involves a technologist who can perform the technical part of the act and who must collaborate or conspire with another individual at the periphery or outside of the computer system who can convert the technical act into gain. It may be a programmer who runs a small computer in a bank for a fictitious day of banking and transfers $100 from each of 41 accounts into an account that his wife has opened under an assumed name. She then proceeds to withdraw the money in small amounts at a time to avoid discovery. In another case, a computer programmer in a large organization wrote a computer program and executed production runs to calculate football pool betting odds for an organized crime ring operating a large number of football betting parlors. The computer programmer was being paid $50 a week and did not know the ultimate purpose of the reports he was producing for his brother-in-law, an intermediary between him and the football betting conspiracy. Vulnerabilities will frequently require persons with different skills, knowledge, and access to take advantage of them.

e. Differential Association

The differential association syndrome is the white-collar criminal's use of small deviations from the accepted practices of his associates. [8] This vulnerability stems from groups of people working together and mutually encouraging and stimulating one another to engage in unauthorized acts that escalate into serious crimes. The competitive nature of technologists in the computer field, and their often elitist attitudes, can result in a one-upmanship competition in performing pranks. The 1973 Ward vs. California case involved the theft of a computer program from a storage of a competing service bureau computer over telephone lines from a batch terminal in the perpetrator's service bureau. [15] A programmer from the victim firm admitted on the witness stand in the associated civil trial that it was common practice for programmers in both of the competing service bureaus to gain access to the other company's computer system for the purpose of playing games or investigating level of use or obtaining the identity of customers and the type of work they were doing. It was determined that the computer in the perpetrator's firm had been accessed in unauthorized fashion by programmers from the victim firm's staff 16 times between the time of the perpetrator's arrest and his trial. This type of vulnerability

CONTINUED

1 OF 5

makes it important for the investigator to interview the associates of possible suspects to determine the degree of differential association that could lead to information about some of the more innocent acts or pranks engaged in that might have led to the more serious alleged crime.

f. Robin Hood Syndrome

Most of the computer-related crime perpetrators interviewed exhibited the Robin Hood Syndrome. [28] They differentiate strongly between harming people, which is highly immoral within their standards, and harming organizations, which they can easily rationalize. In addition, they rationalize that they are only harming a computer or the contents of the computer; therefore, doing no harm or causing no loss to people or organizations. This characteristic is probably common among all types of amateur white-collar criminals and may not be unique to computer-related crime criminals. However, it can be important for the investigator because it may be more pronounced because of the role the computer can play in strengthening the rationalization process. Interviews with computer-related crime perpetrators revealed that they would become quite disturbed if the interviewer even implied, let alone directly accused the individual, that he was a crook in the sense of causing individually identifiable people to suffer losses. A New York City bank embezzler, who engaged in a fraud in his position as head teller, through his computer teller terminal, indicated that he never took more than $20,000 from any one savings account because he knew it was insured to $20,000. Thus, the loss was suffered by the insurance companies and not by his individual customers. [15]

g. Game Playing

This vulnerability is based on the concept that some computer technologists believe that using an idle computer does no harm and that they have a right to use it for personal purposes for challenging intellectual exercise. All but one of the computer-related crime perpetrators interviewed indicated that the attraction and challenge of thinking of their computer-related crime as a game played a significant part in motivating them to continue in their fraudulent activities. Computer technologists tend to be the type of people who like mental challenges and complex game playing. Investigators should anticipate this vulnerability that suspects believe that they are only playing games and they have the right to play games in computers because they have the unique capabilities to do so (the elitist syndrome).

2. Antagonistic Personnel Relationships

The antagonistic and dependent relationships among people in different data processing functions is important for the investigator and prosecutor to know and understand. Among 669 reported cases of

computer abuse [3], collusion was found to be of high incidence; it occurred in one-half of the cases. However, collusion was found to be of low incidence between programmers and computer operators probably because they are in naturally antagonistic functions. Programmers often complain about computer operator's performance in running their programs. Computer operators complain about the practices of programmers that make their programs difficult to run and prone to errors.

Table 19 shows the potential antagonistic relationships among workers in different data processing functions. The information in this diagram can prepare an investigator or prosecutor to deal with people working in different data processing functions. It can be useful to understand the problems that one worker can have in interfacing with another worker. This diagram also implicitly shows in what ways workers in different data processing functions are dependent on workers in other functions.

3. Interviewing Suspects

It is important that investigators fully understand the damage that a suspect computer employee could do in a computing facility. If an employee believes or learns that he is a suspect, he could potentially cause great losses to the victim after the crime has been perpetrated to get even with the victim for reporting him. Logic bombs (see Section I) that might be left inside a computer system represent another danger; even though the suspect could be limited in physical access to a computer, he still could have planted logic bombs that could continue to cause damage at some future time. It is possible that computer equipment vendors could be a source of information about unusual purchases of equipment that might be needed by the computer criminal to perpetrate a crime; for example, the purchase of computer terminals and related equipment by private parties.

It would aid an investigator in conducting interviews to know the various kinds of jealousies, conflicts, pressures, and confidentialities that various data processing people may exhibit. In addition, knowing the few relatively universal characteristics and the constraints on the performance of job situations of computer employees and managers at all levels presented in previous parts of this section may be useful.

It is advisable to run a criminal background check not only on the suspects, but also on the victims. This may be a standard practice in normal investigation, but is particularly important in computer-related cases. Suspects are often willing to talk to investigators because they may see no crime in their activities. Sometimes, they may think their act is unethical or immoral, but not necessarily criminal.

Table 19

POTENTIAL ANTAGONISTIC RELATIONSHIPS AMONG DIFFERENT WORKERS IN DATA PROCESSING FUNCTIONS

	Operators	Programmers	Media Librarians	Data Entry Clerks	Source Data Preparers	Users	Vendors' Maint. Engineers
Operators	From / To ← / Complaints	Job failures, failure to report errors.	Unrecorded removals and submissions			Job failures failure to report errors.	Misuse of equipment Failure to report errors
Programmers	Poor program design. Misleading or absent instructions.		Misleading or absent instructions.	Poor input formats. Poor instructions.	Poor input formats. Poor instructions.	Lack of problem understanding Poor documentation.	Programs Improper use of equipment
Media Librarians	Slow or incorrect media selection.	Loss of media incorrect labelling.				Loss of media	Poor handling of media
Data Entry Clerk	Data errors causing reruns	Data errors unanticipated in program design Program entry errors	Loss of media assigned to them			Data entry errors causing erroneous output	Misuse of Equipment
Source Data Preparers	Data errors causing reruns	Data errors and out of range data not anticipated in program design		Poor legibility on data forms		Data errors causing reruns and incorrect output	
Users	Inconvenient run schedule demands Poor job instructions	Unclear or absent problem specifications. Inconvenient program change demands	Misleading or absent instructions	Inconvenient work schedule demands	Poor instructions. Inconvenient work schedule demands		
Vendors'	Inconvenient equip. maintenance sched. Equip. failures	Equip. failures		Inconvenient equip. maint. sched. equip. failures			

Before confronting or interviewing a suspect, an investigator may find it useful to consider that some prosecutors will not accept a crime case until the victim gives assurance that he will see the prosecution through to the end and be willing to testify. Often, halfway through a long case a victim may decide to accept restitution and drop the prosecution. This wastes the prosecutor's time. In addition, jurisdictional problems often must be settled because of the wide range of geographic constraints and freedoms in on-line computer systems. Many computer systems reside in one jurisdiction but are used from terminals in many other jurisdictions.

SECTION III DISCOVERING THE CRIME

The purpose of this section is to lead the investigator through the unique physical environments of computers, operational procedures, and vulnerabilities in the use of compters to gain the necessary insights and familiarity to be effective in discovering a computer-related crime. The detailed technical concepts of computers are described in Section VI and often are not necessary for effective investigation of many computer-related crimes. However, if technical concepts are at issue, it is advisable to obtain expert assistance. The methods of investigation after discovery and dealing with evidence are discussed in Section IV.

The discovery topic, which omits investigative and scene search methods known to experienced investigators, is addressed in two ways. The first three subsections present the operational, physical, and computer usage environments that the investigator will encounter. The last subsection describes the weak points that are susceptible to criminal acts in computer centers. This provides the investigator with ideas on where and what he might look for in crime discovery.

A. COMPUTER OPERATIONS

An operations center can function in many different organizational configurations. Typically, however, its two major divisions are: production support and equipment operations.

1. Production Support

The production support group often is concerned with several activities. Each is capsulized below.

a. Data Capture

Data capture consists of two steps. The first step is the physical gathering of data from sources such as orders, time clock cards, sales slips, recordings, or electronic sensors. After they have been gathered, the data must be converted into machine-readable form. Thus, the second step is data conversion.

The conversion of source data may occur at an operations center, or at originating (user) departments, and may take several forms. The data may be: punched into cards or paper tapes; keyed onto magnetic tape, disks, diskettes, etc.; typed or printed onto sheets or cards to be read by an optical character recognition (OCR) or MICR reader; or keyed directly to a computer.

To detect errors that may have occurred in the keying of data, a second operator may key the same data using the same medium used by the first operator (i.e., paper tape, magnetic tape, magnetic disk, or

punched cards) so as to determine differences, if any, in the way the two operators keyed the data. The differences are resolved and, if necessary, corrected data are prepared.

Manual checking methods are generally used to edit or verify the significant data on input that are typed on to sheets to be read by an OCR.

b. Scheduling and Coordination

As its name implies this function, establishes and maintains production schedules, monitors the production job stream, and makes adjustments as necessary. It also provides a point of contact for users, helps them enter jobs, and expedites work through the operations center.

c. Job Setup and Control

The job setup and control function is often part of the scheduling and coordination function. It handles individual jobs as they enter, flow through, and leave the operations center. Controls are established and maintained; jobs are logged in; inputs are reviewed and edited as required (by the systems designer and user); jobs are made up by assembling job control cards, materials, and files; and outputs are reviewed and prepared for distribution.

d. Library and Services

These services maintain the tape and disk library and other operations libraries and provide support services (such as supplies inventory) to the operations center.

These functions are sometimes found in equipment operations rather than production support, particularly when jobs originate and are output at a remote teleprocessing terminal. In such a case, the library responds to instructions relayed to it by the operating system rather than the job set-up and control unit.

2. Equipment Operations

The equipment operations/computer processing group is concerned with several activities. Each is capsulized below.

a. Data Preparation

Data preparation usually means putting the machine-readable records in the proper sequence called for by the program and also to perform editing and validation functions to ensure that the input meets certain criteria, such as balancing to users batch total or checking that certain fields contain only numeric or only alphabetic characters; or that values in certain fields are within prescribed limits; or that the

codes in certain fields are consistent with the codes in other related fields. Putting data records in sequence or merging them with other records can be performed by many different types of equipment. For example, a punched card sorter/collator system is efficient, but it is slow compared to a computer. A file of 2,000 cards can be read on to magnetic tape or disk in about 1 minute. A computer program then can sort the records in their proper sequence in a few seconds. A program can also contain instructions for editing the data during the sorting operation, thus minimizing the errors that could occur through the physical handling of cards.

b. Computer Processing

After data have been edited, the next steps are computer processing and output of data. Processing and output generation are susceptible to two types of errors: program and equipment. The use of flowcharts and careful programming can prevent most program errors. After a program has been written, debugging and testing detect the more subtle errors so the program will perform as intended. A computer itself can be programmed to identify some programming errors. For example, an instruction to divide by 0 is an invalid command that most computers will detect. If such an error is detected, a computer will generally stop processing that particular program and go on to the next program. The operator then either corrects the error or notifies the user to supply a remedy.

Computer circuitry malfunctions are rare because modern electronic circuits and components are extremely reliable. Computers are now so nearly error-free that an undetected failure resulting in erroneous output almost never occurs. Some more recently designed computers have built-in error detection and correction circuitry to overcome internal faults that would have shutdown an earlier computer; they even keep a record or log of errors so that maintenance personnel can replace faulty parts. Regularly scheduled maintenance of the computer also keeps failures to a minimum--that is, to ensure efficient functioning without expensive, time-consuming errors and reruns.

Operator mistakes can occur during any phase of data processing. Precautions taken to ensure error-free input, effective and efficient programs, and reliable equipment can be nullified if the computer operator makes a wrong decision, mishandles materials or data, or is careless in operating the system. Valuable time can be lost, and an entire job may have to be rerun. But the cost of a rerun may be the least costly alternative in some applications. For example, in billing customers, it is usually far more important that the bills be accurate than sent out at a certain time. Accordingly, comprehensive and complete system operating instructions must be provided so that both the computer and terminal operators can follow the operations schedule and ensure proper turnaround time and processing consistency for each job. These instructions, often referred to as a run book, must be precise and

explicit and should describe: operations set-up procedures, job schedule checklist, action commands, error correction and recovery routines, input/output (I/O) dispositions, and system backup procedures. These system operating instructions will vary according to the size and type of the installation. However, the following is representative of a standard run book's contents:

- o Operations Set-up Procedures: This procedure includes logging on to the system with the run date, time, and terminal control numbers.

- o Job Schedule Checklist: Listed here are the run frequency, processing deadline, run time, retention periods for I/O files, and scheduling priority of the jobs.

- o Action Commands: Computer-generated instructions and commands are given that call for operator responses to make the system perform a specific action.

- o Error Correction and Recovery: The operator will follow these procedures to enter optional override messages designed to bypass halts or properly suspend processing due to abnormal job termination. System restart procedures are also included.

- o Input/Output Dispositions: This section addresses the disposition of input and output data from the remote and central sites.

- o System Backup Procedures: Remote and central site backup procedures provide an alternative processing method in the event of computer, program, or operator malfunction. These procedures include, but are not limited to, re-assignment of peripheral and terminal devices.

In a remote job entry (RJE) environment, these procedures should be augmented by local (remote) procedures for data collection, inquiry, batch transmission, and data reception scheduling. These procedures should specify the availability of data, scheduling priorities, frequency of transmission, and transmission times, as well as remote backup procedures.

In summary, it is the responsibility of the systems designer and the user to determine jointly the parameters within which a computer operator may be allowed to continue processing after some condition occurs that halts processing. The specific actions that an operator is to take are generally incorporated in a run book (or a step-by-step procedure for the operator). Deficiencies in the run book, which must take into account all of the probable conditions that may occur during the processing of an application, are often the weakest link in the chain. This is so because of the initial urgency connected with getting

the system operational, or because changes that are made to the application program are not reflected in the run book. In either case, the result may be to halt the system and delay processing, or worse, to allow processing to produce faulty output. For all of these reasons, comprehensive tests are undertaken at the initiation of a new application, or change to an application, to determine whether controls and operator instructions are adequate.

c. Storing and Accessing Data

Computer data files can be classified in various ways. They can be classified according to the method of accessing the data contained in the file or by the purpose the file serves. For batch applications, files can either be sequential-access or direct-access; whereas, on-line, real-time applications are almost always direct-access (see Section VI for the meanings of these terms). Additionally, a file may function as a master, transaction, or output file.

Sequential-access devices store and release data in sequence, one record after another; whereas, direct-access devices store and release data from any part of the medium as directed by a computer program. Direct-access devices also can be used for sequential-access processing.

Card readers, punched-tape readers, optical and magnetic-character readers, and magnetic tape drives are sequential-access devices. They handle only sequential data.

A magnetic tape has data recorded or magnetized on one side, and the tape drive has a stationary read/write head that either reads data from or records it onto the tape as the tape passes over the head. In a typical computer operation center, a master tape file may be mounted on one tape drive, a transaction tape file on another tape drive, and an output tape file on a third tape drive. The central processing unit would determine, from the program stored in computer memory for that application, what data to write onto the output file from the data contained on the master and transaction input files.

In a direct-access environment, magnetic disks and drum drives are the direct-access devices. They can provide access directly to individual records in any order.

A disk pack consists of several metal plates or disks mounted on a vertical shaft that spins the disk pack. A computer writes or reads data on the disks in much the same way as it would on magnetic tape except that old data are lost as new data are written over them (the same as a dictation recorder works). As data are put onto a disk, a table of contents is built to provide information about the file, including the physical location of the record on the disk. With this arrangement, a computer can find records that have become obsolete or need changing without searching through the entire file (as must be done in a sequential-access tape processing system).

Generally speaking, direct-access devices are more expensive than sequential-access devices because of the complexity in providing greater speed, versatility, and capacity. The difference in cost, however, may be justified by the nature of the applications to be processed. Regardless of the choice of storage type, most computer operation centers back up their files with copies on tape; and where disk files are used, the disk file is usually copied on to tape to be safely stored as a backup. Then the tape can be used to restore the disk file if necessary.

Magnetic files not only store more data per unit of physical size than paper files, but also are more susceptible to damage. Tapes can be crimped or stretched, and disk packs can experience read/write head crashes onto the magnetic surface.

Safety storage measures that are appropriate for paper are often inappropriate for a magnetic medium. Paper burns at 451 degrees F; the glue that binds ferrite particles to tapes and disks melts at temperatures as low as 125 degrees F. Consequently, a fire-retardant vault that protects paper may provide only limited protection for tapes and disks.

d. File Retention and Backup

In view of the vulnerability of data stored on a magnetic medium, adequate file retention and backup are crucial. More files are damaged by human error than by disaster or sabotage. It is safe to assume that unintended "erasures" are a prime cause of data loss on tape files. When correct actions are not taken, valid data tapes are erased because some data centers still use unlabeled tapes.

Labeling tapes, however, does not prevent accidents. Most operating systems have an option that permits a retention date or period to be placed in the internal label. This option often is not used, and thus the operating system cannot detect tapes that should not be erased. With some operating systems, even when a retention period is specified in the label, the operator can ignore the console warning message and write over a tape that should have been saved.

Updating the wrong edition of the file can also destroy data. For example, the operator can mount the wrong edition of the file and ignore any warning messages from the operating system. The user may then fail to notice the problem when reviewing the reports.

Updating problems can also occur when there is more than one transaction tape during an update period. One tape may be used more than once or not at all. Unless the user has externally generated control totals, such operational errors can be difficult to detect.

On-line systems present another problem because there may be no record of the input. If a disk file is accidentally destroyed, reconstruction may be impossible unless a tape or another disk copy of the input is made during the data capturing operation.

Program as well as equipment malfunctions can also destroy or alter files to the point where the data are unusable. Files can also be destroyed by human errors. Tape reels and disk packs are delicate. If someone grasps an unprotected tape reel by the outer edge rather than at the hub, the tape can be crimped such that it is unreadable. Similarly, dropping a disk pack can render the data it contains unusable.

These and other operations problems can destroy or degrade files to the point where it is necessary to reconstruct them. Reconstruction, in turn, requires file backup.

Whereas operational problems usually destroy a single file or a limited number of files, disasters can destroy an entire library. Fire is probably the most common natural disaster facing a data center. In a sense, a computer center creates its own fire hazards--high voltages and highly combustible paper dust.

e. Storage Location for Backup

All data centers have files stored in the computer room and/or an adjacent tape library. These on-site files may be inside a fire-retardant tape vault or safe, but more frequently they are on open shelves in a room that may be protected by automatic sprinkler systems. When a safe or vault is used, the operations manager may not use off-site storage--believing that the vault provides adequate protection. As previously discussed, this may not be true; off-site storage can often enhance file security. Because off-site storage is intended to provide protection against disaster, off-site facilities are usually far enough from the on-site facility so that one disaster will not destroy both locations.

f. Testing the Usability of Backup Materials

Although the standards may stipulate updating procedures for backup programs, the procedures may not be properly followed. Moreover, although the standards may indicate which master and transaction files are to be stored off-site, the schedule may not be kept. The standards, therefore, normally include a procedure for testing the backup. For example, backup programs and files are usually used annually; problems and failures are noted, and the standards are modified as necessary.

3. Typical Reports Generated by a Computer System

Computer operation management requires reports on many operational functions. These are usually produced automatically by the computer system. The following list indicates some of the types of reports that are produced and their frequency in a typical operation.

Computer Operator Console Log (Frequency: Continuous)

Chronological listing of computer system events and operator actions. Identification of tape reels and disk packs mounted, systems programs used; assignment of job numbers to particular users, commencement and termination of specific jobs, and use of system resources, such as a line printer. Directs impromptu operator actions; most comprehensive listing of computer system events.

Machine Room Access Log (Frequency: Continuous)

Chronological description of all persons gaining access to the machine room. If visitors are admitted, their escort is also identified. Identification card/badge readers are often used to record this information.

Processing Schedule (Frequency: Daily)

Explicit processing schedule (run book) showing the time at which specific jobs should be run. Lists files to be used for the identified jobs; files are specified by tape number and date created. Applications and systems programs to be executed are delineated by program identifiers and accounts to be charged. Files may or may not be stored on magnetic tape reels.

Daily Detail List (Frequency: Daily)

In-depth report of users accessing the system, the log-on and log-off times of these users, their priority codes, and accounting data relating to computer system resources consumed. Accounting data includes CPU time, I/O activity, and connect time. Errors and warnings concerning accounting data, such as an invalid job order number, appear here.

Computer Utilization Summary (Frequency: Daily, Weekly, Monthly, Year to Date, as Requested)

Extracts data from Daily Detail List to perform statistical analyses. Provides a breakdown of ways in which computer was used: hours on-line, amount of time the processor was idle, I/O activity, etc. May be presented by user, job order, application program, project, or division. Helpful in the detection of unauthorized use of system resources.

Computer Utilization Accounting Control Report (Frequency: Weekly)

Relates statistical data set forth in Computer Utilization Summary to accounting charges made during this period. Shows total dollar accounting units for CPU time, I/O activity, and the like.

Valid Job Order List (Frequency: Weekly)

Describes job orders that are currently recognized and to which jobs may be charged. Jobs may originate within the organization or through a telecommunications network; accounts to which either may be charged are listed here.

Accounting Code Error Listing (Frequency: Weekly, Monthly)

Sets forth time, user, and other circumstantial details of errors in job order codes, user IDs, and the like. An aid in the detection of browsing and searches for accounts to which unauthorized activities may be charged.

Computer Utilization Summary by Priority Code (Frequency: Monthly, Year to Date)

Description of ranks assigned to tasks that determine the precedence in which jobs receive system resources. Broken down by projects, divisions, locations, or users. Shows disproportionate uses of system resources.

Terminal Usage Report (Frequency: Monthly, Year to Date)

Details usage, as measured by connect time, for specific terminals. May contain the times at which a terminal was in use.

Computer Storage Summary (Frequency: Semiannually, as Requested)

Provides a measure of on-line storage used by specific job orders. May also contain information on off-line tape reels and disk packs associated with a job order.

4. Computer Products and Supplies

Many companies supply computing equipment and related supplies and services. These companies distribute their products and services throughout the nation, usually through a network of sales and service offices and/or agents. The local offices of these companies can be contacted by consulting the white pages of a telephone directory, and they will be able to answer most inquiries.

Typically, the larger computer manufacturers offer a wide range of products and services covering nearly everything a computer user might need. Many smaller companies selectively compete in just one or a few of these product areas. Nearly all computer installations use multiple vendors, sometimes many.

Equipment manufacturers affix to each machine a permanent tag showing the manufacturer's name, the unit serial number, and other information, such as time or place of production. The information from

this tag is sufficient to identify the supplier in most cases, thereby enabling the user to contact the equipment manufacturer to answer any inquiry regarding the functioning of the equipment.

Other items, such as software, supplies, and services cannot be so readily tracked to their source. Inquiries must usually be addressed to the data processing professionals in the organization who are often familiar with their department's use of all such supplier-provided items and can provide the supplier's name and address.

B. PHYSICAL FACILITIES FOR COMPUTERS

What one may see in a large data center regarding the efficient use and protection of its assets will vary considerably from center to center. These variances are a function of top management's perception of the importance of the data center to its business, and according to that judgment, what it is willing to invest to properly use and secure these assets as opposed to what it is willing to risk. Clearly as businesses differ, so do the needs for data processing. A business oriented to handling a huge number of transactions will probably have a large data center to process its work. However, the degree to which operating control measures are imposed therein often depends not on how much is to be processed, but on how sensitive the transactions are to the business. For example, a bank will obviously have a greater need for control than a mail order house where the value of each sale is very low. Similarly, the extent to which one may or may not adopt different types of control, security methods, mechanisms, and procedures will vary by the size of the business, its economic strength, and how it may be regulated by government or other auditing agencies.

Because of the great number of differences among data centers, it is not possible to cover all of them in this discussion. Therefore, what follows is a description of a large, idealized data center with need for comprehensive operating control and security. From this, scaled-down versions can be applied for data centers whose needs are less critical. This description is provided to guide a layperson in a computer center. Computer centers do not all necessarily have all of the features described here.

1. Protection Facilities

Fire protection and detection, annunciation panels, mantraps, guard stations, access control devices, telephone, and internal communication procedures and devices are common elements in an effective operation.

Fire Protection and Detection -- Fire protection and detection cover several considerations. These include the number, kind and location of fire alarms, fire extinguishing equipment, fire department notification methods, the use of nonflammable and nontoxic materials, and the cables and wiring that are used in the data center.

Annunciation Panels -- Annunciation panels are used to signal abnormal conditions. These include fluctuations in electrical power, water detection, fuel levels in power generators, status of coolant pumps, unauthorized entry and intrusion alarms, and the like.

Mantraps -- Mantraps are usually double doors at computer room entrances with doors activated by security guards inside the guard station. They often include keycard door locks, burglary alarms, closed-circuit TV surveillance, magnet and metal detectors. A mantrap generally functions to help the security guards detain a person attempting to enter or leave the computer room until the guards are satisfied that the person is authorized to be there and presents no threat to the center.

Guard Stations -- A guard station is a specially constructed and designed enclosure that is usually connected to, or part of, the mantrap. Often, these stations are manned 24 hours per day, 7 days per week and are equipped to monitor the security of the data center through TV monitors, public address speakers, direct manual alarms to the police, private security service and fire departments, intercoms with the data center, bulletproof walls, doors, and windows, TV surveillance and automatic photographing of persons entering the mantrap, radio police scanners tuned to emergency channels, walkie-talkies for emergency communications, and sometimes a wide array of automatic shutoff switches to reduce harm to the equipment in the event of detection of some abnormal function occurring within the center.

Access Controls -- Access controls often are card-key locks, automatic door closing, fingerprint identification and other means of logging in, cameras trained on entrances, hallways, loading docks, elevator doors, outside building entries, and potentially vulnerable public access areas above, below, and around the data center. These also might include mirrors to eliminate blind spots in these same areas and emergency lighting units to be turned on in the event of failure in the regular lighting system.

Internal Communications -- Internal communications include intercom systems among guard stations and all areas concerned with the daily operation of the data center. Generally, the systems provide the guards with override capability of all stations, conference calling capability, and busy line indicators. As mentioned above, direct communications lines with police and fire department are often provided, as well as walkie-talkies and public address systems to all data center areas.

Telephone Service -- The telephone system installed must be reasonably secure against wilful or accidental damage. Consequently, the wiring of the system is often under the raised floor, encased in fire protective materials, and equipped with smoke and heat detectors. Generally, several lines are used in the event that one becomes inoperable.

2. Technical Computer Safeguards

A list of computer safeguards would be endless. There are several books that list many of them. [19, 29] An investigator or prosecutor will encounter them in any case of suspected crime, and he should ask the victim to have all safeguards that were or could have been involved described and documented. Technical safeguards in computer systems include data file protection, storage partitioning, protected or privileged mode for operating system programs, encryption, exception reporting, and access control.

An example of a comprehensive computer-related safeguard shows the complexities needed. It is password access control in on-line, multiaccess computer systems where access to the computer through terminals must be controlled by verifying the identity of the terminal user on the basis of a secret password he knows. An effective password capability normally has the following characteristics:

- Passwords are of sufficient length to reduce the possibility of guessing.
- Passwords are based on a random selection of characters and assigned to the password holder rather than letting him chose his own password which would be too easily guessed. However, it is also claimed that it is better to allow users to choose their own passwords so that nobody else will know it.
- The password being typed into the terminal is not visible to other people in the area nor is it visible on any printed paper coming from the terminal. Many computer terminals provide for this capability.
- Password holders are periodically indoctrinated about the secrecy of their passwords.
- Safe password administration is required. This includes imposing need-to-know restrictions on password lists, frequent password changes, separation of duties in the administration of passwords, accountability for the safety of the passwords, and background investigation of those people in the high positions of trust who administer.
- The password lists stored in the computer and used for authorization purposes are encrypted using secret coding techniques. As soon as a password enters the computer from a terminal, it is immediately encrypted in the same fashion and compared against the master password in encrypted form only. This reduces the exposure of actual passwords in the computer.

- Time delays are imposed on terminal users so that attempting to use unauthorized passwords repeatedly requires discouraging amounts of time. Also, an individual is not allowed to input an incorrect password more than three times.
- The usage of all passwords is journalled in the computer system. The data files produced are then analyzed by the computer and exception reports produced that indicate deviations from normal password use that might indicate attacks on the system.
- Procedures are established for imposing alternative methods of security when the password system and the computer equipment supporting it fail to function properly.
- Sanctions are clearly known by password holders, and violators are punished.

If a password system does not include at least all of these characteristics, it is probably not an adequate safeguard.

3. Operation and Production Areas

The principal component of the operation and production areas to be considered in data center design are the computer room, operation center, libraries and vaults, and the vendor service engineer area. These are described below.

Computer Room -- Because the computer room is the heart of the data center, it is designed for effective, reliable, and low-risk operation. This implies that it is located away from any mechanical and electrical rooms and within the building at a location that would avoid flooding or water main breaks and yet enhance access for fire fighting. The shell of the secure computer room usually has a fixed ceiling and door of steel and concrete construction and steel and concrete walls that are fire-resistant for a 2-hour minimum. Usually, the computer room has no windows or skylights; in the event that it has, they are permanently sealed and fit with appropriate alarms.

The most common type of floor is the raised or free access type. Raised floors serve several practical purposes. Cables placed under the raised floor do not obstruct aisles. Air-conditioning conduits to computer components may be ducted under the raised floor, or the entire space may serve as a plenum with conditioned air under pressure directed to vents to components. Each panel of the floor, usually 24 inches square, is removable for access to the space below. The distance between the subfloor and the raised floor usually ranges between 15 and 24 inches. The floor panels are guaranteed against static buildup and easily cleaned.

The layout of the computer room is designed for production flow for work movement, permit sufficient aisle clearance for handtruck or equipment, and provide sufficient space for equipment maintenance. Traction pads are installed on all ramps to prevent slippage. Printers and card devices are located for the most convenient access to supplies; however, such peripheral equipment is usually located away from the tape drives and electronic devices because of the paper dust these devices generate. Fire extinguishers are both strategically located for easy access and frequently inspected. Signs indicate the type of fire extinguishers that can be used and how to use them. Similarily, other signs are placed in critical areas to instruct everyone on the use of other safety devices such as power cutoff switches and evacuation routes.

Operation Centers -- The operation center is a room generally used for production control, scheduling, and user coordination. Although it often is located inside a computer room, the operation center should be situated elsewhere because traffic and security problems should be minimized in this area. It may also be adjacent to the guard station so as to provide the surveillance, protection, and communications that are available from these stations.

Libraries and Vaults -- Libraries and vaults generally are located just off the computer room, and only one entrance is provided directly into the computer room. The same steel and concrete construction prevails here as in the computer room, and similiar alarm devices and surveillance methods are used. The humidity and temperature controls, however, are separate or independent from the computer room and have a backup capability in case of failure of the main system. The floor supports in this room generally require greater strength because of the use of safes and other heavy containers. Safes are usually rated to ensure their proper use; that is, as indicated earlier, some safes will adequately protect paper documents but are not sufficient to protect magnetic tape media. Safes sometimes also have automatic safe door closing in the event of fire or other emergency.

Vendor Service Engineer Area -- The vendor service engineer area is located away from the computer room and general traffic flow thereto, but it usually is within easy access of the computer room. The computer and peripheral equipment vendors engineers who maintain the computer system are located here along with the spare parts and test devices for the system. Leakproof, lockable, fire-proof cabinets are used to store a minimal supply of cleaning solvents necessary to maintain equipment.

4. Mechanical and Electrical Support Facilities

Several mechanical and electrical support facilities are found in the data center. These are briefly discussed below.

Electrical Power -- Because a data center is totally dependent on electrical power, it receives special attention. Separate areas for mechanical and electrical equipment rooms to store equipment necessary for daily processing operations and for emergency backup are provided away from the computer room. Some of the types of equipment that are stored in these rooms include: uninterruptable power supply (UPS) such as batteries, diesel generators and control circuitry; fuel tank for diesel generator; motor generator for CPUs; water chillers; spare fuses and fuse panels; and other spare parts and tools. The rooms are equipped with floor drainage with backwater valves, smoke and heat detection, water sprinkler systems or Halon (R) gas fire suppression systems, CO and water fire extinguishers properly placed, humidity and temperature indicators and controls, bypass switches for emergencies and maintenance, devices to record variations in input power, transformers specifically for the data center, watertight outlets beneath the floor, and all of the surveillance and communications previously mentioned. Most important, the data center electrical system is separate from other building facilities and means are provided to back up this system when required. These rooms have an inconspicuous location requiring infrequent access by facilities engineers.

Lighting -- Artificial lighting is provided throughout the data center because of few if any windows. Aside from the requirements of candle power, which will vary by area, there is provision for emergency (battery-powered lights) throughout the data center, in the mechanical and electrical equipment rooms, and in critical surveillance areas. These are connected to the annunciation panels and able to be controlled from inside the guard station.

Air Conditioning -- Although the need for air conditioning in data centers is an obvious requirement, it frequently is not adequate to produce a reasonably trouble-free environment. Too often the air conditioning that supplies the building is also used to supply the data center; however, the needs for an office environment, or any other kind of environment, usually are quite different from those required by a data center, and therefore air conditioning for a data center is usually separate and provides for a backup capability. The air conditioning satisfies not only the requirements of the equipment, but also the numbers of personnel who might be used to operate the equipment. Additionally, special air intake devices are used to protect against noxious fumes or corrosive materials entering the environment. Air filters conform to UL Class 1 and are easily accessible for inspection and replacement. Several portable temperature and humidity recorders are located throughout the data center. Critical spare parts are stored on site.

Motor Generators -- Some central processing units (CPUs) require motor generators to provide a level and quality of power different from standard commercial power. Spare units are on hand to back up primary units, and these are equipped to automatically cut over in the event of a primary failure. They are located to provide easy access for on-site repair, maintenance, and manual testing and sufficient capacity to be able to take a unit off-line without service interruption. They also are connected to annunciation panels and other signal devices to warn of potential damage.

Water Chillers -- Like motor generators, some CPUs require water chilling equipment to provide a constant appropriate temperature. The same backup protection that applies to motor generators applies to water chillers.

Uninterruptable Power Supply -- A UPS system provides electrical power to the data center if there is a commercial power failure; it also allows a return to commercial power or other separate power sources. Because it provides power for computer equipment, lighting, telecommunications, motor generators, annunciation panels, security controls, security equipment, and other means of automatic entry and exit such as doors and elevators, the UPS system requires weekly testing of the entire system. The UPS system also provides protection against unexpected surges in power that might otherwise damage the system (data processing equipment).

5. Other Areas Related to the Data Center

Several other areas are related to the data center. If a reception room for visitors and users exists, it is located outside the data center. Pickup stations for delivery or pickup of materials are adjacent to other data center areas. Elevator shafts are not common to any walls of the computer room or other data center rooms or critical areas. If an elevator is necessary, its use is restricted to data center personnel or authorized personnel, and is connected to a monitoring system in the guard station when the elevator stops at the data center level. Operators' lounges are frequently provided, particularly in installations that have 12-hour shifts. Preferably it is not accessible except through the data center in that its purpose is to provide a rest area inside a data center so that operators can remain on the premises.

Janitorial rooms have central access to the data center so that adequate cleaning and maintenance may be performed in an efficient manner. Because various cleaning supplies are stored and these rooms are generally equipped with deep sinks, it is important that these rooms

are protected against fire and water damage and the extension of that damage to the data center. Accordingly, these rooms are constructed in much the same way as the computer room (except for the raised floors) and have the same kinds of protection devices to monitor against potential damage.

Locker rooms and rest rooms have common access to each other, but are not located adjacent to the computer room or any critical mechanical and electrical equipment rooms or facilities. Nevertheless, because these rooms obviously must be reasonably close to the data center, it is important that they have a public address system and protective devices against fire and water damage. For the same reasons, these rooms have no windows or other means of access that would present vulnerability to the data center.

Storage and supply rooms are used to provide materials for efficient operation. It is particularly important to note, however, that these rooms are not located next to the computer room or mechanical and electrical equipment rooms because the materials they contain often are combustible. For this reason, these rooms have intercom stations, fire extinguishers, water systems that are independent of all other data center areas, floor drains with backwater valves, water alarm connections to annunciation panels, and intrusion alarm systems to signal entry that is monitored by the guard station. These rooms therefore have fire-proof cabinets to contain solvents, cleaning agents, or other materials that are potentially combustible.

C. COMPUTER USAGE

1. Computer Usage in Science and Engineering

The first computers were designed and built for the solution of extensive mathematical problems. ENIAC (Electronic Numerical Integrator and Calculator), developed during World War II for the computation of weapons ballistic schedules, was the first all-electronic calculator. [30] From these early beginnings, computers have become a basic computation tool of the scientist, the design engineer, the astronomer, the architect, and the weather forecaster.

Scientists are trained and experienced in the methods for defining and solving the quantitative problems encountered in their professional fields. In many cases, these solutions have been previously developed into computer programs which are made available to the user for a fee. The scientist need enter only the variables associated with his case in the form required by the computer program, and the solution is computed and returned to him. In other cases, the scientist develops his own computer program for the solution of a newly encountered problem or a

previously solved problem in a new or preferred way. This computer program, often considered a proprietary secret by the scientist's employer, is used for the solution of one problem or a series of similar problems.

Scientists, mathematicians, engineers, and others being trained in the quantitative disciplines today are taught to use the computer as a problem-solving tool. They are usually taught several computer programming languages and when and how to use those skills. Their background is usually college education and advanced degrees in the physical, life, and social sciences and engineering.

The scientist often uses a programmable calculator or a small specially designed computer for some of his problem-solving work. In other cases, he shares the use of a larger computer with other users. When a larger computer is shared, it is necessary to isolate each user's computer programs and data from all other users. The scientific user is given a unique password that he uses to store his private data files in the computer and subsequently gain access to the data and/or programs. This is done by a special computer operating control program that controls the access of users' information stored in the computer. The user can access only his own private store of information.

The scientist/engineer computer user is usually working independent of programming assistance toward the solution of his problem and deals directly with special, programmed systems stored in the computer for his use. Typically, he does not need to communicate with any person in computer services to do his work. Exceptions occur when the process fails or when new kinds of problems develop.

2. Computer Usage in Organizations

The organizations of our society--the businesses, governments, and other bodies--do much of the work and employ most of the work force. Hence, they account for the largest number of users of computers today.

Unlike the engineer/scientist, a production or operational member of an organization is dependent on others for information and procedures that are essential to the conduct of his work. Others in turn are dependent on him. Seats cannot be reserved on a flight until someone, probably far removed from the reservation clerk, has scheduled the flight and entered it into the computer. Reservations cannot be confirmed unless all reservations previously made are known to be entered.

The organization is typically concerned with efficiently processing the large amounts of information it often deals with. The bank, the retail merchant, the telephone company, the police department, the

airline, and the census bureau, all depend on effective information processing. The computer has become the dominant means for meeting the diverse information processing needs for these and many other kinds of organizations. This need to process large amounts of information through a computer effectively and efficiently has fathered the development and growth of the information processing specialist.

Colleges and universities have responded to this need with a specialized curriculum, known as Computer Science, to train and develop candidates for the information processing field. Persons trained for other positions in government and industry are offered computer-related courses such as introduction to computers and basic programming skills to acquaint them with the use of computers; these courses, however, do not offer the advanced information processing techniques contained in the Computer Science curriculum.

The important role of computers has led to the development of departments specializing in computer systems within the various organizations of our society. This computer systems department is given the responsibility for developing effective and efficient computer systems to meet the information processing needs of the organization. Typically, the top management of the organization determines where computers can be used advantageously, funds the new activity, and hires a staff of specialists to conduct the work of developing and operating the computer systems. Hence, the organization is in a position of dependence on specialized skills and knowledge on the computer systems department. The computer systems department supplies information processing services to other departments that use that service to perform their work.

The organizational user of computer services interacts with the computer systems department in several ways. Usually he deals with staff in the section of the computer systems department that operates the computer and performs the information processing. He deals less frequently with people in the section that develops or changes the computer systems, including systems designers and systems programmers.

Virtually all large organizations use computer services to process their payroll information; to compute the gross and net pay and issue checks or make deposits; to compute and record the related information, such as payments due to governmental entities, credit unions, and so on; and to supply the information necessary for organization compliance with the various laws and agreements governing salaries and wages. The payroll example illustrates the respective roles of the computer systems department and the computer services user.

The payroll department typically collects the time cards or other proof of wages due, checks to make sure they are properly signed, and develops a batch control such as number of time cards and an arithmetic

total of the total hours shown on the cards. The batch of time cards then goes to the computer operations where the data entry operators record the information from the time cards into a computer processible form, such as punched cards, magnetic tape or disk. These cards or equivalent records are then processed by the computer to develop a proof list showing the content of each record and containing arithmetic control totals that correspond to those developed in payroll. The two sets of control numbers are compared either by a control function in computer operations or in the payroll department. Computer operations is not authorized to proceed with the payroll process until all differences are resolved to the satisfaction of the payroll department manager.

This type of check and balance is used throughout a well-designed payroll system to ensure that the payroll department has full control over the operations done for them by the computer services department. This design approach gives the payroll department the necessary authority to see that its responsibilities are carried out fully and accurately.

A second kind of interaction develops when it is necessary to change the payroll processing system or to produce a new one. The change may be as minor as a new withholding schedule for social security or as major as a new labor contract requiring the development of entire new pay computing and reporting procedures. In either case, the payroll department works through the computer systems development department to create the new systems or to change the existing system.

Other reasons for reprogramming the payroll program may be complexity caused by frequent modification or to take advantage of more cost-effective equipment and methods. For example, programs have so many changes made to them that their complexity increases, efficiency drops, and documentation becomes obsolete. There are too many instances when documentation becomes so poor and the program so complex that the programmers who can successfully change or correct them dwindle to one, or even none are left. This represents poor management practices, but frequently happens. Many large computer programs are so complex that no individual comprehends the whole, and all errors or bugs are never found and corrected. Therefore, a computer program needs continual care and maintenance, and its output can never be totally trusted under all input variations.

In this relationship, the payroll department also retains full responsibility for the completeness and accuracy of the resulting process. Payroll must be satisfied that the system it receives from systems services meets the need. Because payroll personnel cannot read and understand the computer programs that make up the computer system, they must rely on an audit of the results obtained from a real or theoretical trial or test of the system. These results are obtained in

a process known as a "test run." In the test run, the computer performs the various processes in the new or revised system against a sample of information that will produce a known answer if the system is correctly programmed.

Examination of real examples of payroll and computer services departments working together on systems will quickly reveal that the results developed from the interactions are not perfect. Rather, they reflect the organization environment as well as the abilities and knowledge, or lack thereof, of the persons involved in the design and operation of the systems. Control steps are often overlooked or bypassed in the haste to make deadlines, or simply left out of the system design to save money.

To meet other deadlines, new or revised systems are often put into operation before testing is completed, sometimes with disastrous results. Seldom, if ever, do the users, designers, and programmers of systems foresee and provide for all possible eventualities. Seldom also do systems tests seek to verify the results from all parts of the system acting both alone and together.

Computer systems suffer the shortcomings common to all systems designed, built, and operated by man. The computer, like other machines, will faithfully perform as instructed when kept in good working order. However, the computer receives its processing instructions and raw material in the form of unprocessed data from people and is therefore only one of the parts of a payroll or any other system.

3. Computer Application Systems Design and Development

Computer application systems are an arrangement of human and computer methods, procedures, and processes arranged to work together as a unified whole to produce a prescribed result. New systems begin with a "system design" that specifies the parts of the system and defines how they will fit together. These designs are typically done by a systems analyst as described in Section II. Design begins with an investigation to define the needs to be met and to determine the resources available. The systems analyst works with the computer service user departments to define their information processing needs. He then determines the human and other resources, including the computer resources, required to meet those needs. These human, computer, and other resources are incorporated in a system designed to meet the users needs.

The resulting system design is documented in a manner designed to ensure effective and efficient execution of the system development phase and to assist with the subsequent installation, operation, and maintenance of the system. Systems development is typically done by the systems analyst and one or more application programmers (see Appendix D). The programmer codes the several computer programs that will become

part of the final system, tests these programs against a set of sample information to make certain they perform as required, and corrects them as necessary in a process known as "debugging." The final stage of program testing includes installing all the programs on the computer and running them in a full production mode to make certain they perform as planned. This step is known as the "systems test."

Few systems design and development projects follow these steps from beginning to end without some reversion to a previous stage. Systems design is often found faulty during programming, and programs often fail to mesh properly when the systems test is done. In these and similar situations a part of the system is taken back to the design stage for a partial redesign and/or reprogramming phase. This process is continued until satisfactory results are obtained.

The applications programmer works closely with the systems analyst, assisting him during the development of the system. He codes and tests programs in accordance with the systems design, prepares test data and tests them, participates in the systems test, recommends systems design changes to improve the system, and prepares the completed program for installation in the computer operation. He also documents the programs in accordance with his employer's standards.

The programmer's task begins with a definition of the form and source of the data to be processed and the form and content of the results required usually supplied by a systems analyst (Programmer/analysts serve in both capacities). The programmer analyzes this information to determine the specific steps the computer will have to perform to produce the required results. The results of this analysis are often recorded onto a flowchart using drawn boxes joined by flow lines that shows the overall design of the program and is used as a road map during the coding of the program. Frequently the flowchart, again like a road map, does not predict the detours encountered on the journey, and at journey's end does not provide a record of the route actually followed.

When the flowchart is developed and recorded, the required computer steps are written onto paper in a form that is acceptable to the rules and conventions of a programming language. It is possible to code directly into the machine language used by the computer, but easier-to-use and quicker languages have been developed that rely on a program to translate the programmer's code into machine language. Section VI.B.3 on Programming Languages describes the different types of languages and uses of each.

When the program coding is completed, the programmer-coded statements are converted into machine-readable media such as punched card, magnetic tape, or magnetic disk. The converted and machine-readable program is called a "source program."

Newly coded programs are seldom if ever perfect. Therefore, programs are tested and debugged before they are used on a production basis as stated above. The test is conducted by running many variations of data through the program, including some erroneous data. The results produced by the test run are checked and analyzed to determine whether they conform to the defined requirements of the program. If they do not, the programmer modifies the source program code and repeats the testing procedure until satisfactory results are achieved.

The final stage of program development is documentation. Program documentation includes a collection of the information useful and necessary to the future use, understanding, and where necessary, modification of the program. Complete program documentation usually includes:

- o Narrative -- a document describing the purpose of the program and the general solution used.
- o Logic display -- a description of the significant logical steps in the program, often a flowchart.
- o Program listing -- a printed copy of the source program. These copies are normally produced by computer.
- o Input/Output formats -- a description of the data files and reports showing the relative location of each field in each record.
- o Test data -- a copy of the test data used to debug the program.
- o Operator instructions -- the instructions necessary to run the program on a computer. The format and content of these instructions are specified by the organization and vary widely from company to company.

The section of the computer services department that is responsible for designing and developing new computer application systems and for revising existing systems to meet new needs is usually called "systems and programming" or "application systems development." Most employees of such departments are engaged in either designing systems or writing computer programs or both.

Computer systems design and development organizations vary with the size and complexity of their responsibilities. The small and limited computer installation may depend entirely on vendor-supplied and purchased systems and will often have just one or two systems employees who devote their time to testing and installing these systems. The large and comprehensive computer installation may employ hundreds of systems design and development personnel. Typical organization structures by size are summarized below.

Small Systems Departments -- These departments typically consist of several persons, each reporting to the computer center manager. These persons each perform all the tasks necessary to design and develop systems; the computer center manager would often do a part of the systems design and development work.

Medium Departments -- Medium-sized departments typically contain at least one manager or supervisor reporting to the computer center manager. This person is responsible for the programming work and perhaps the systems analysis and design also. Specialization between systems design and programming also begins at this stage. Systems programming also appears as a specialty, reporting either to the programming manager or the computer operations manager.

Large Departments -- The specialization first encountered in the medium-sized department is extended further in the large department usually to include manager and staff devoted to systems analysis and design, a separate manager and staff specializing in applications programming, and a third department specializing in systems programming. Additional specialists, including technical writers, training and education personnel, librarians, and standards personnel, also appear in very large sections. The several department managers may report to the computer center manager or to an intermediate manager of systems and programming.

Large systems projects usually require the participation of several specialties. Staff from the several departments are often assigned to work together on project teams to conduct this work, usually under a project leader who is typically the most experienced member of the team, often a senior systems analyst. The project team carries the project through to installation and successful operation of the system. The team is then disbanded, with its members returning to their respective specialty organizations and a program maintenance team takes over.

D. COMPUTER SYSTEM VULNERABILITIES

For effective investigation and prosecution of computer-related crime, many vulnerabilities seem obvious, but it is easy to overlook some of them--even the important ones. Therefore, two analyses are presented, based on the principal vulnerability found or surmised in each of 362 recorded cases of computer abuse. [27] The first analysis was based on a breakdown of common functional weaknesses, such as inadequate I/O controls; the second was based on a breakdown of the most common functional and physical locations of vulnerabilities. The results of the analyses of these two categories of computer system vulnerabilities are discussed below.

1. Functional Vulnerabilities

Eight primary functional vulnerabilities to computer abuse emerged from analysis. They are listed in Table 20 and summarized below in order of frequency of occurrence. Each vulnerability is general enough to maintain an acceptable level of confidence in assignment of cases to types of vulnerabilities. This approach was adopted because the amount of information about some cases is limited. Examples from the file that demonstrate the range of acts facilitated by each vulnerability appear in Appendix D.

Table 20
VULNERABILITIES TO COMPUTER ABUSE BY FUNCTION
(Incidence in Reported Cases)

Vulnerable Functions	Number of Cases	Percentage of Cases
Manual handling of input/ output data	147	41
Physical access to EDP facilities	46	13
Operations procedures	43	12
Business practices	41	11
Computer programs usage	33	9
Operating systems access and integrity	24	6
Time-sharing service usage	19	5
Magnetic tape storage	9	3
Total	362	100

Poor Controls over Manual Handling of I/O Data -- This vulnerability from poor controls over manual handling of I/O data was associated with 147 cases. The greatest vulnerability occurs wherever assets are most exposed. During the past 17 years--the period of reported cases--assets have been most tangible and subject to human acts before entry into computers and after output from computers. Data

assets are more accessible outside computers than when they are within them, and programs must be executed to achieve unauthorized access. Controls that are often absent or weak include separation of data handling and conversion tasks, dual control of tasks, document counts, batch total checking, audit trails, protective storage, access restrictions, and labeling.

Weak or Nonexistent Physical Access Controls -- This access vulnerability to computing facilities accounted for 46 cases. Where physical access is the primary vulnerability, nonemployees have gained access to computer facilities, and employees have gained access at unauthorized times and in areas in which they were unauthorized. Perpetrators' motivations have included political, competitive, and financial gain. Financial gain occurred mostly through unauthorized selling of computer services, holding computer centers for extortion purposes, burglary, and larceny. In a number of cases, employee disgruntlement has been the motivating factor. In some of these cases, disgruntlement stemmed from frustration with various aspects of automated society. Controls that were found to be weak or nonexistent include door access, intrusion alarms, low-visibility of assets, identification and establishment of secure perimeters, badge systems, guard and automated monitoring functions (closed-circuit television), inspection of transported equipment and supplies, and staff sensitivity to intrusion. A number of the intrusions occurred during nonworking hours when safeguards and staff who might notice intrusions were not present.

Four cases in which abuse was facilitated by physical access vulnerability involved attacks on computers with firearms. One case involved a dispute over national politics, and two are presumed to have involved citizens frustrated in dealing with government bureaucracy and computer-based services. The fourth case was perpetrated by a computer operator frustrated with his job.

Computer and Terminal Operational Procedures -- This vulnerability accounted for 43 cases. Losses from weaknesses in operational procedures have resulted from sabotage, espionage, sale of services and data extracted from computer systems, unauthorized use of facilities for personal advantage, and direct financial gain associated with negotiable instruments in operational EDP areas. The controls whose weakness or absence facilitates these kinds of acts include separation of operational staff tasks, dual control over sensitive functions, staff accountability, accounting of resources and services, threat monitoring, close supervision of operating staff, sensitivity briefings of staff, documentation of operational procedures, backup capabilities and resources, and recovery and contingency plans. The most common abuse problem has been the unauthorized use or sale of services and data. The next most common problem is sabotage perpetrated by disgruntled EDP operations staff.

Weaknesses in Business Ethics -- Abuse facilitated by this vulnerability accounted for 41 cases. A weakness or breakdown in business ethics can result in computer abuse perpetrated in the name of a business or government organization. The principal act is related more to a company's practices or management decisions rather than to identifiable unauthorized acts of individuals using computers. These practices and decisions result in deception, intimidation, unauthorized use of services or products, financial fraud, espionage, and sabotage in competitive situations. Controls include review of business practices by company board of directors or other top level management, certified public accountant audits, and effective practices of regulatory and law enforcement agencies.

Weaknesses in the Control of Computer Programs -- This vulnerability from weak control of computer programs facilitated 33 cases. Programs are assets subject to abuse. They can also be used as tools in the perpetration of abuse and are subject to unauthorized changes to perpetrate abusive acts. The abuses from unauthorized changes are the most common. Controls found lacking include labeling programs to identify ownership, formal development methods (including testing and quality assurance), separation of programming responsibilities in large program developments, dual control over sensitive parts of programs, accountability of programmers for the programs they produce, the safe storage of programs and documentation, audit comparisons of operational programs with master copies, formal update and maintenance procedures, and establishment of ethical concepts of program ownership.

Operating System Access and Integrity Weaknesses -- This vulnerability in access and integrity of operating systems facilitated 24 cases. All of these record compromises of computer operating systems involve the use of time-sharing services. Compromises are accomplished through discoveries of weaknesses in design or taking advantage of bugs or shortcuts introduced by programmers in the implementation of operating systems. The acts involve intentional searches for weaknesses in operating systems, or the unauthorized exploitation of weaknesses discovered accidentally. Students committing vandalism, malicious mischief, or attempting to obtain computer time without charge have perpetrated most of the acts in university-run, time-sharing services. Controls to eliminate weaknesses in operating systems include methods for proving the integrity and security of the design of operating systems, imposing sufficient implementation methods and discipline, proving the integrity of implemented systems relative to complete and consistent specifications, and adopting rigorous maintenance procedures.

Poor Controls over Access Through Impersonation to Time-Sharing Services -- This vulnerability from impersonation to time-sharing services facilitated 19 cases. Unauthorized access through impersonation to time-sharing services can most easily be gained by obtaining secret passwords that are keys for the most common method of protecting users of time-sharing services. Perpetrators learn passwords that are exposed accidentally through carelessness or administrative failures, or obtain them by conning people into revealing their passwords or by guessing obvious combinations of characters and digits. It is suspected that this type of abuse is so common that few victims bother to report cases in recordable form. Control failures include poor administration of passwords, failure to change passwords periodically, failure of users to protect their passwords, poor choices of passwords, absence of threat monitoring or password-use analysis in time-sharing systems, and failure to suppress or obliterate the printing of passwords.

Weaknesses in Magnetic Tape Control -- This vulnerability in magnetic tape control accounts for 9 cases. Theft of magnetic tapes, their destruction, and data erasure from them are acts attributed to weaknesses in control of magnetic tapes. Many other cases, identified as operational procedure problems, involved the manipulation of data on tapes and copying. (No cases are known in which magnetic disk packs have been subject to abusive acts.) Controls found lacking include limited access to tape libraries, safe storage of magnetic tapes, the labeling of tape reels, location and reel number accounting, control of degausser equipment, and backup capabilities.

2. Functional Locations of Vulnerabilities

The functional locations of vulnerabilities to computer abuse were analyzed for the 362 cases. Data and report preparation areas and computer operation facilities--the physical locations with the highest concentration of manual functions--were the most vulnerable locations.

Nine primary functional locations of vulnerabilities emerged from the analysis. Table 21 lists the location of vulnerabilities, and they are summarized below.

Table 21

VULNERABILITIES TO COMPUTER ABUSE BY FUNCTIONAL LOCATION

Vulnerable Functional Locations	Number of Cases	Percentage of Cases	Total Number of Cases	Total Percentage of Cases
Data and report preparation	120	33		
Terminal areas	14	4	134	37
Computer operations	95	26		
Terminal areas	10	3	105	29
Non-EDP	44	13	44	33
Computer systems	7	2		
Terminal systems	33	9	40	11
Programming	27	7	27	7
Magnetic tape storage	12	3	12	3
Total	362		362	100

Computer Data and Report Preparation Facilities -- The data and report preparation facilities were the locations of 120 cases. Areas included key-to-tape/disk/card data conversion, computer job setup, output control and distribution, data collection, and data transportation. Input and output areas associated with on-line remote terminals are excluded here.

Computer Operations -- Computer operations were the locations of 95 cases. All functional locations concerned with operating computers in the immediate area or rooms housing central computer systems are included in this category. Detached areas containing peripheral equipment cable connected to computers and computer hardware maintenance areas or offices are also included. On-line remote terminals (connected by telephone circuits to computers) are excluded here.

Areas Without EDP Functions -- Forty-four cases occurred in non-EDP locations. Many cases involved business decisions in which the primary abusive act occurred in non-EDP areas such as management, marketing, sales, and business offices.

On-Line Terminal Systems -- The on-line terminal systems were the locations of 33 cases. The vulnerable functional areas are within on-line computer program operating systems where acts occur by execution of programmed instructions such as are generated by terminal commands.

Programming Offices -- Programming offices were the locations of 27 cases. This includes office areas where programmers produce and store program listings and documentation.

Data Preparation and Output Report Handling Areas for On-Line Terminals -- Fourteen cases occurred in data preparation and output report handling locations. This category includes the same functions identified in the first discussion of data preparation facilities, but is associated here with on-line terminals rather than computers.

Magnetic Tape Storage Facilities -- The storage facilities for magnetic tapes were the locations of 12 cases. Areas included in the category are tape libraries and any storage place for tapes containing usable data. This does not include temporary or short-term storage of tapes in tape-drive mounting areas. The latter are included in categories discussed above on computer operations and computer data preparation facilities.

On-Line Terminal Operations Areas -- The on-line terminal operations areas were the locations of 10 cases. This category is the equivalent of the computer operations discussed above, but is in on-line terminal areas.

Central Processors -- The central processors were the locations of 7 cases. These functional areas are within computer systems where acts occur in the computer operating system (not induced from terminals).

3. Accidental/Intentional Losses

Errors and omissions occur generally in labor-intensive functions in which people are involved in detail work. The vulnerabilities occur where detailed, meticulous, and intense activity requires concentration. The vulnerabilities are usually manifested in data errors, computer program errors (called bugs), and damage to equipment or supplies. This requires frequent rerunning of a job, error correction, and replacement and repair of equipment or supplies.

It is frequently difficult, however, to distinguish between accidental loss and intentional loss. In fact, some reported intentional loss comes from perpetrators discovering and making use of errors that result in their favor. When a loss occurs, data processing employees and managers tend first to blame the computer hardware because this would absolve them from blame, and the problem becomes one for the computer vendor maintenance personnel to solve. The problem is rarely a

hardware error, but proof of this is usually required before the source of the loss is searched for elsewhere. The next most common area of suspicion is in the user department or at the source of data generation because, again, the data processing people can blame another organization. Next, blame tends to be placed on the computer programming staff. Finally, when all other targets of blame have been exonerated, data processing employees will suspect their own work. It is not uncommon to see informal meetings between computer operators, programmers, maintenance engineers, and users arguing over who should start looking for the cause of a loss in his area. The possibility that it was intentionally caused is even more remote from their thoughts because they assume they function in a benign environment.

People in many computer centers do not understand the significant difference between accidental loss from errors and omissions and intentionally causes losses. Organizations using computers have been fighting accidental loss for 35 years since the beginning of automated data processing. They have anticipated the unthinking things that people do. Solutions are well known and usually well applied relative to the degree of motivation and cost-effectiveness of controls. On the other hand, they anticipate that the same controls used in the same ways will also have an effect on people engaged in intentional acts that result in losses. They frequently fail to understand that they are dealing with an intelligent enemy who is using his greatest skills, knowledge, and access capabilities to solve his problem or reach his goals. This presents a different kind of vulnerability that is much more challenging and that requires adequate safeguards and controls not yet fully developed or realized, let alone adequately applied.

4. Natural Forces Vulnerabilities

Computer systems clearly are vulnerable to a wide-range of natural as well as man-made forces. Table 22 lists most of the forces that can cause damage and destruction. Computer systems and facilities are fragile, and intruders can find great leverage using simple methods to engage in malicious mischief, arson, vandalism, sabotage, and extortion with threats of damage. Natural events from extreme weather and earth movements can also be used by an intruder to achieve his destructive purposes.

In the 1960s, magnetic fields were identified as a major source of potential attacks. Tests performed at the National Bureau of Standards indicated that the erasure of magnetically recorded data on tapes and disks does not pose a significant problem because the field strength of a magnet deteriorates rapidly with distance. A number of alleged crimes in which individuals used magnets to erase massive amounts of magnetically recorded data were found to be myths and never occurred. There is a small danger that a magnetic tape or disk might be placed near enough to a source of a magnetic field to cause erasure. Such

Table 22

NATURAL FORCES CAUSING VULNERABILITIES

Extreme temperature		
Hot weather	Cold weather	Fire
Gas		
War gases	Commercial vapors	Humid air
Steam	Wind	Tornado
Explosion	Smoke	Dust
Liquids		
Water	Rain	Flood
Ice	Snow	Sleet
Hail	Chemical solvents	Fuels
Projectiles		
Bullets	Shrapnel	Powered missiles
Thrown objects	Meteorites	Vehicles
Earth movements		
Collapse	Slides	Flows
Liquefaction	Shaking	Waves
Cracking	Separation	Shearing
Electromagnetic discharges		
Electric surge	Electric blackout	Static electricity
Microwaves	Magnetism	Laser
Atomic radiation	Cosmic waves	

fields could be generated by large electric motors or generators. A magnetic tape placed in an exact spot on the floor of a subway car in New York City over the location of the electric motor could cause some erasure.

One of the few verified cases of use of a magnet to destroy data occurred in a New York City office in 1962.[15] A disgruntled employee used a hand-held magnet against the coiled edge of a magnetic tape through the flange window of the reel. He was successful in erasing one bit position closest to the edge used to check errors. The data contents of the tape were still readable. A large hand-held magnet would normally have to be placed within a fraction of an inch of the recording surface to have a significant impact.

Most computer centers possess a degaussing (demagnetizing) device for the purpose of erasing magnetic tapes. It is about the size of a portable electric heating plate for cooking. Degaussers should normally be kept under lock and key or at least located in a different room or area from that where magnetic tapes may be stored.

Computers can also be affected by radio frequency energy that might emanate from a radar antenna. This is usually solved by putting a conductive, grounded screening material in the walls around a computer (Faraday cage). It has been reported that radio frequency emanations normally produced by a computer system can be monitored by sensitive radio receivers and used for espionage purposes. This is found not to be the case except where one piece of computer equipment is sufficiently isolated from all other computer equipment, such as a terminal located 20 ft or 30 ft away from other equipment. However, the cost of the monitoring radio receiver makes this kind of crime most unlikely except possibly in military systems.

SECTION IV MAKING THE CASE

This section is designed to aid in the practical application of technical knowledge of computers to the case development and prosecution of computer-related crime. Section V addresses the applicability of the law to such crime. Because investigators and prosecutors are assumed to already be trained in investigative and prosecution techniques, this section focuses only on those aspects requiring application of computer technology, the computer environment, job responsiblities (including management), computer operation, and security provisions described in previous sections.

Prosecutors and investigators should avoid becoming overwhelmed by the complexity of computer technology by applying their knowledge and experience from other criminal cases, obtain only necessary technical information from experts, and translate the technical aspects into terms more familiar to the criminal justice community. The technical aspects should be subordinated to the typical crime facts as much as possible. However, there is the danger in court that confusion over technical matters may lead to reasonable doubt and a lost case. In fact, the defendent may be well aware of this point and emphasize the technical complexity. This requires that the prosecutor be fully prepared to deal with technical matters and to avoid or simplify them when possible in his own case presentation.

When a prosecutor attempts to introduce computer-related evidence in a trial, the greatest care must be taken to prove its authenticity and relevance. A technically knowledgeable defense attorney often can effectively prevent the court's acceptance of such evidence. This can be done by confusing the court in technical complexity and obscurity or by challenging the integrity of the material or its production. The integrity and freedom from error in operation and use of a computer can easily be challenged successfully unless great care and detailed, competent monitoring is performed by people at every step of the process. The prosecutor may have to match his experts against those of the defense; therefore, the more knowledgeable and competent experts who have been more directly involved in the evidence-producing processes and who are the more effective witnesses on the stand will prevail.

A team approach to a complex computer-related case is desirable. An investigator, a DDA, a computer expert, and an EDP auditor would make an ideal team. The capabilities and roles of experts and auditors are presented in Section II of this manual.

Investigation should be well advanced when possible before an arrest is made, exhibits obtained, experts consulted, search warrants and affidavits completed, witnesses interrogated, and subpoenas prepared. As stated in Section II, there is a great danger that the investigation will alert the possible perpetrators and thereby allow them time to obliterate evidence, which can often be done with ease in a computer environment. This must be taken into account in determining the degree, type, and secrecy level of an investigation.

A. LEGAL DEFINITIONS IN COMPUTER TECHNOLOGY

Foreknowledge of computer technology in the law can be useful to prosecutors in considering the various aspects of a computer-related crime case. The application of this information in the development of a case is discussed below.

One of the traps a prosecutor may face is the challenge to his claim that a computer was involved in an alleged crime that would make a computer crime law applicable. Basic advice is to minimize the computer's role and prosecute on the basis of the criminal law most familiar to the prosecutor and the court. For example: theft of a computer program might be prosecuted as a simple copyright law violation. It may not be reasonable to make the case for a program theft that involves definitions of what constitutes a computer program and what constitutes taking it from a computer storage device in object form or in uncompiled form in source code.

Therefore, the preparation of a case involving computer technology should include a careful consideration of the identification of the technical aspects of the case. This should include computers and computer programs if they are involved to ensure that the technical aspects of the case fall within the definitions of the law to be applied. It may be useful to refer to testimony, studies, and supporting or opposing statements made at the time the law was enacted to make the meanings and intent of the definitions clear.

1. Definitions of Computers

Consider the range of definitions of computers found in current or proposed state laws as follows:

- Florida: Computer means an internally programmed automatic device that performs data processing. Computer system means a set of related or connected or unconnected computer equipment, devices, or computer software. Computer network means a set of related remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities.

- Arizona: Computer means an electronic device that performs logical, arithmetic, or memory functions by the manipulations of

electronic or magnetic impulses and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in the system network. Computer system means a set of related, connected or unconnected computer equipment, devices and software. Computer network means the interconnection of communication lines (including microwave or other means of electronic communication) with a computer through remote terminals or a complex consisting of two or more interconnected computers.

- California (proposed): Computer system means a machine or collection of machines used for governmental, educational, or commercial purposes but excluding pocket calculators that are not programmable or access external files, one or more of which contain computer programs or data that performs functions including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control. Computer network means an interconnection of two or more computer systems.

- Illinois (proposed): Computer means an internally programmed general-purpose digital device capable of automatically accepting data, processing data, and supplying the results of the operation. Computer system means a set of related, connected devices including the computer and other devices, including but not limited to data input and output, storage devices, data communications links and computer programs, and data that make the system capable of performing the special-purpose data processing tasks for which it is specified.

- Utah (proposed): Computer means any electronic device or communication facility with data processing ability.

It is clear that within any of these definitions a computer or computer system could be a giant IBM 370/168 computer system occupying several large rooms to any device containing a microprocessor chip such as a digital watch, microwave oven, electronic game, or every automobile to be manufactured starting in 1981.

In one definition, a computer must be internally programmed. Historically, the term "internally programmed" has been used to differentiate a computer from a calculator where all of the instructions are manually entered one at a time and would be considered an externally programmed device. However, the algorithm (set of rules) for performing multiplication and division are automatic, internally programmed functions that would make a calculator internally programmed as well. Another definition of this term might be that the computer program must be generated internally to the device rather than the typical process of writing computer programs on coding forms, keying them into computer media, entering them into the device, and starting the device to follow the instructions in the program. Under this interpretation, no devices could be defined as a computer except those that automatically generate

their own computer programs--a highly unlikely possibility in today's technology. Some computers have been programmed to be self-learning and construct their own programs to solve problems. However, the programs that perform the self-learning have been written externally and placed in the computer.

It is possible that charges in an alleged crime may refer to computer when computer system or computer network is meant, or it could refer to computer system when only an isolated computer is involved. Therefore, charging will have to be done carefully to match the definitions of computer and computer systems.

Other problems appear when computer is defined as an electronic device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses. It may be argued that a word processor system does not perform logical, arithmetic, or memory functions but performs functions on words and symbols and stores such words and symbols in a storage device not covered by the term "memory functions." The definition also states that it includes all communication facilities that are connected or related to such a device in a system or network. If a computer is on-line to the dial-up telephone system, this means that all the telephone systems in the world and all the computers in the world connected to the telephone systems become part of the computer. It might be argued that these definitions are so broad as to make the law so unspecific that it becomes meaningless.

Some of the definitions include software or computer programs among the parts of a computer system or computer. In most cases, computer programs (using the less ambiguous term) are not considered a part of the computer, but are entered at the time when data processing is to be performed. Some more advanced computers have permanently installed computer programs, and others have computer programs semipermanently installed (sometimes referred to as firmware). Differentiation of the meaning of software and programs may be made between the computer operating system programs that normally must be present in a large-scale computer to make it function on a practical basis and application programs that perform problem solving. However, this distinction is not made in the definitions.

The definition of a computer in the California bill states that a machine or collection of machines is a computer system only if it is used for governmental, educational, or commercial purposes. This would exclude or include computer systems depending upon their particular use. A computer owned by an individual and used for hobby or amusement purposes would not be covered by the proposed law, whereas the same computer, if used by a small business, would be covered by it.

2. Definitions of Computer Programs

Computer programs have been defined in the various state bills and laws as follows:

- Florida: Computer program means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data. Computer software means a set of computer programs, procedures and associated documentation concerned with the operation of a computer system.

- Arizona: Computer program means a series of instructions or statements in a form acceptable to a computer which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer systems.

- California: Computer program means an ordered set of instructions or statements or related data that when automatically executed in actual or modified form in a computer system, causes it to perform specified functions.

- Illinois: Computer program means a series of coded instructions or statements in a form acceptable to a computer which causes the computer to process data in order to achieve a certain result.

Computer software is a jargon term used in the computer field that has a variety of definitions. Software sometimes refers to a computer operating system; at other times refers to any computer program; and at other times, as in the definitions above, includes the documentation that could theoretically include huge volumes of documents including the computer user manuals, electronic circuitry schematics, all input that has ever been used with the program, and all output that has ever been produced by the use of the program.

A computer program is often thought of as only computer instructions. Computer programs often contain considerable amounts of data that are used as constants, tables or parameters, and are part of the program. According to some of the definitions when a program is executed by a computer, it causes the computer to process the data. Computer programs could be written and used that do not process data but only perform some logical function, such as setting electronic switches. There are also some computer programs that look like ordinary English language text. Other computer programs could be written in the form of graphical diagrams or tables of data.

B. COMPUTER EVIDENCE CONSIDERATIONS

As in the preparation of any case for prosecution, the use of evidence is a significant element.

The most likely of the principal defense strategies that will arise in a computer-related crime case will be an attack on the admissibility of the prosecutor's computer or computer-generated physical evidence. He should be alerted that perhaps in no other type of crime is an attack on admissibility of evidence more likely to succeed. The purpose here is to alert prosecutors to those potential evidence issues based on general law principles that are most likely to be used in computer-related crime cases and to encourage that preventive measures be taken during all investigative and prosecutive stages.

1. Search and Seizure

The nature of computer-related crime investigation frequently will require a search of a computer center or a remote computer terminal location, either as the situs of the crime or of the fruits of the crime. Equally likely will be the necessity to seize computer or computer-generated physical evidence as essential evidence for successful prosecution.

Thus, an entire pandora's box of legal issues becomes available to the defense, and the alert prosecutor must remain ever mindful of this potential. The nemesis here is the exclusionary rule that could well obliterate the prosecutor's case. Most search and seizure issues, such as consent, informers, entry, and searches incident to detention and arrest generally will arise and apply much as they would in noncomputer-related cases.

In computer-related crime cases, search warrants should generally be obtained and used. Special consideration should be given, however, to situations providing application of exigent circumstance exceptions to preserve evidence because of the high degree of ease with which both imstruments and fruits of the crime can rapidly destroy or alter computer evidence. Application of the plain view doctrine should be cautiously relied on. There is a strong likelihood that a defense will attempt to show the lack of sophistication of most prosecutors and investigators in computer technology.

Furthermore, avoid reliance on the use of an expert informant at the search scene to point out what items should be seized. California prosecutors are directed to People vs. Superior Court (Williams) 77 C.A. 3d 69 at page 78 for a discussion of this issue. Another problem with informers is that generally they will be insiders and are legally 'untested' or 'unreliable' as informers. Thus, be prepared to show sufficient corroboration of their information before preparation of the warrant or the search.

A difficult problem in drafting computer-related search warrants will be the tightrope walk between 'reasonable particularity' in describing the items to be seized. Avoid, as much as possible, the necessity of seizing items not described in the warrant. A data processing expert will be necessary in drafting the warrant to ensure that all system hardware and program components are included.

The timeliness of the execution of the warrant may be critical. The avoidance of legal staleness of the information or other time constraints imposed by law is one objective balanced against the need of the prosecutor to obtain evidence of an operational fraud--i.e., a fraud that occurs only during an actual computer operation. The problem becomes more difficult when the operational fraud arises out of irregular computer usage.

Many more search and seizure 'traps' may await the computer-related crime prosecutor. Therefore, be open to using imagination and ingenuity as well as the training and experience obtained in all computer-related search and seizure situations.

2. Obtaining Evidence

When a search calls for obtaining documents, they can be visually identified and computer technology expertise is not usually needed. Documents such as system manuals, computer run books, interpreted punch cards (with printed contents across the top), program documentation, logs, data and program input forms, and computer printed forms are usually labeled as to their contents. Whether they are complete, original, copies and match search needs can be determined by careful and complete questioning. Lack of cooperation of hostile custodians of documents may be overcome by separate questioning of individuals.

Requesting program documentation may require knowledge of computer program concepts to know the types and extent of documentation required--e.g., source listing, object listing, flowcharts, test data, storage dumps, etc. It must also be realized that program documentation is frequently obsolete relative to currently used versions of the programs. The latter must be obtained in new computer printouts. Program documentation is usually found in a centralized library. However, in some programming organizations the most recent documentation is in the possession of individual programmers and must be obtained from them or their offices. If there is any question about what may be obtained or identified, an expert should accompany the search officer.

Taking possession of other computer media materials may be more technically complex. Magnetic tapes and disks are normally externally labeled as to their contents, but a log or program documentation may be necessary to obtain full titles or descriptions given only the reel number or coded label. The program documentation must be for the program that produces or uses the tape. A large tape file may reside on

more than one reel of tape (called volumes). It may be necessary to have a trusted technologist check the contents of a tape or disk by using a compatible computer and computer program.

Searching for information inside a computer can be highly complex and requires experts (see Section B.3. for details). Preparing a search warrant for this also is complex and requires expert advice. Any materials that must be seized may also be required for continued operation of the computer center. If the intent is not to inhibit continued operation, a copy of the material may have to be made. If the copying is to be done at the searched facilities, a trusted person should be assigned to the task. It may be easy to destroy information before it can be removed; however, if it is destroyed in a computer center, there frequently will be backup copies stored in a remote backup facility.

The California Evidence Code now states that computer-generated evidence is the same as traditional evidence. However, the reliability and integrity of the computer-generated evidence must be proved. Computer-generated evidence can be the result of the work of several different technologists, including the systems analyst who designed and specified the computer program that produced the evidence, the programmers who wrote and tested the programs, the computer operators who operated the computer to run the programs that produced the report, the data preparations staff who prepared the data in computer-readable form (tape or disk), the tape librarian with the responsibility for supplying the correct tapes or disks containing the source data, the electronic maintenance engineer who maintains correct function of the hardware, the job setup clerk and job output clerk who are responsible for manual handling of the input and output before and after the job is run, and the system maintenance programmer responsible for the integrity of the computer operating system used in the execution of the computer program.

It is better to use a generally known, accepted, and widely used computer program package as evidence rather than to have a special-purpose program developed or have some other special-purpose program that may be in the victim's possession. Generalized EDP audit packages are available from several program vendors and CPA firms (see Appendix F). These programs should be used whenever possible. Logs and journals that provide records of the execution of the program should be obtained and initialed by the individuals responsible for the actions that result in these records.

The security efforts in safeguarding can be an important aspect in the investigation and prosecution of a suspected computer-related crime. If a computer organization has a security specialist (see Section II), he can be of great assistance in providing information concerning deviations from normal activities that might be associated with a suspected crime. His records could provide significant amounts of evidence that might be used in a criminal trial, primarily because they

may be an exception to heresay evidence rules in that the records will frequently be produced in the normal course of business. The computer security specialist can quickly and easily brief an investigator or prosecutor on the safeguards that may be associated with or violated in a computer-related crime.

A computer security office may have some of the following information files of use to the investigator.

- Audit reports filed by date and subject that could reveal vulnerabilities and problems.
- Computer operations exception reports of checkpoint restarts, missing tapes and output, data communications traffic errors, password and access failures.
- Loss experience reports of accidental and intentional acts.
- Assets lists including all computer equipment and programs, data files, supplies, and facilities.
- Floor plans of all facilities.
- Maintenance records of safeguards and controls.
- Personnel summary files and listings.

There may be a problem, however in convincing a victim to give up important evidence in the form of magnetic tape reels of master files and various materials needed to continue the business. This problem might easily be solved by having the victim make and use copies of the material. The prosecutor must be sure that he obtains the original material and not the copy because he would otherwise have to establish the integrity of the copying.

The EDP auditor within the victim organization or from the external CPA organization that audits the victim organization can be of great help in assuring the integrity of the methods used in obtaining evidence. As stated in Section II, their function is to ensure the integrity of all data processing for victim organizations. The professional societies that these various auditors belong to often have certification programs and codes of ethics that may be used to assist in validating the integrity of the technologists who may be used.

Much can be gained from the negative experiences and complications of obtaining and introducing computer-related evidence in trials. This can be an aid for advising the potential victims of computer-related crime of the kinds of controls and safeguards that they should install to result in acceptable evidence in cases of these kinds. Examples of safeguards are the labeling of computer programs and data, journaling of computer system activity, audit trails built into systems that result in reports that can be categorized as ordinary business reports, and retention of potential evidence for a reasonable period of time.

3. Computer Reports as Evidence

Data contained in the storage devices of a computer or in computer-readable media such as magnetic tape, punch cards, punch tape, removable disks, or electronic plug-in storage devices are frequently needed as evidence in human-readable form. Accomplishing the printing or display of data does not normally result in erasing or destroying the data in the computer or computer-readable media unless that is the intended purpose. However, if desired in this process, the storage device or media can be erased, the contained data replaced with other data, or physically destroyed, or made unusable. Normally, only copies of the desired data are obtained. The report production process is described in Figure 1. Occupations of people who participate in real-time and nonreal-time modes in the production of a report are also indicated. (Detailed job descriptions are provided in Appendix D.) This is important for the prosecutor who may need the testimony of such people to validate the integrity and correctness of the report-producing process.

a. Production Steps in an On-line System Mode

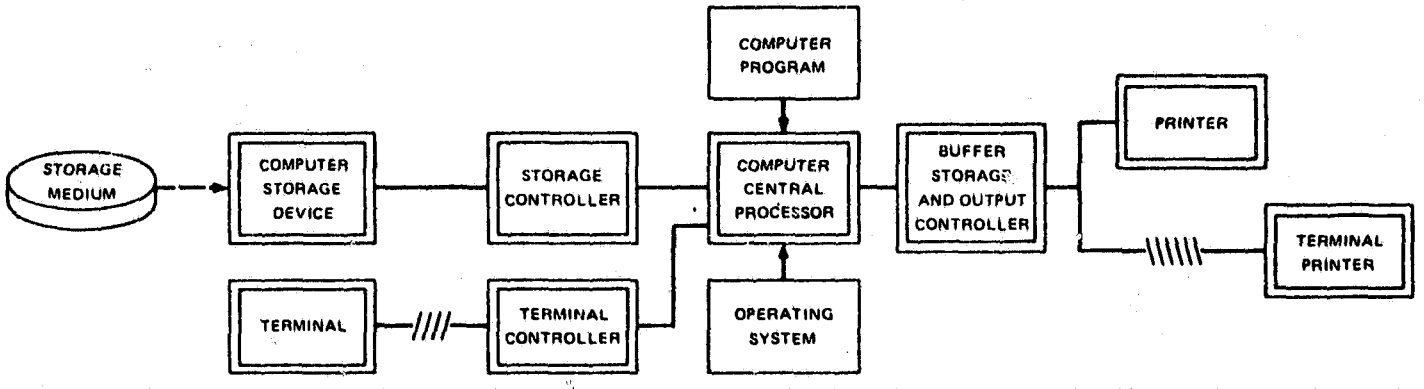
In an on-line system, it is possible to obtain the report in two ways. The report may be produced at a terminal, or it may be requested from a terminal but printed at the computer site and delivered to the requester. (See Appendix F for time-sharing usage examples.) The steps in either case are as follows:

(1) Log on to an activated terminal with authorization and identity codes.

(2) Enter the system mode providing user interaction with the data file of interest.

(3) Request a copy of the data file or part of it by specifying its name, using formatting instructions and commands. This will cause the proper file to be accessed if it is on-line. If it is not available, a message will appear on the computer console printer or CRT informing the computer operator of a request for an off-line file. The computer operator will take action to make the file available in on-line mode. This may require assistance of a media librarian and a peripheral equipment operator. In the case of a magnetic tape file, the tape must be retrieved from the tape library adjacent to or near the computer peripheral equipment and mounted on a tape drive. The tape drive must be assigned with an address (usually a single digit). The address is either specified by the computer or must be typed into the console typewriter for the system to locate the source of the file.

(4) The file or selected part of it will be displayed on a CRT, printed on a printer at the terminal or printed at the computer site, and delivered to the user according to the commands entered at the terminal.



REAL TIME PERSONNEL	MEDIA LIBRARIAN	PERIPHERAL OPERATOR	JOB SETUP CLERK	COMPUTER OPERATOR	PERIPHERAL OPERATOR	JOB OUTPUT CLERK	TERMINAL OPERATOR MESSENGER	
NONREAL TIME PERSONNEL	EQUIPMENT MANUFACTURING WORKERS	INSTALLERS TRANSPORTERS	FACILITIES ENGINEERS	MAINTENANCE ENGINEERS	SYSTEM PROGRAMMER	APPLICATION PROGRAMMER	AUDITOR SECURITY SPECIALIST	

FIGURE 1 PRODUCTION PROCESS FOR COMPUTER REPORTS

b. Production Steps in an Off-line System Mode (Batch Processing)

In a system where the data retrieval is to be performed in batch mode, the steps outlined below are normally performed.

(1) The user fills out a form to be key-punched on cards or directly prepares punch cards with the user identification and authorization information, file name, formatting instructions, and retrieval commands. The forms, cards, and file media (if in the user's possession) are submitted as a job at the computer service desk or proper receptacle.

(2) The job setup clerk puts the job request cards in a stack with other jobs and delivers them with file media or file media request forms to the computer operator. He obtains necessary file media such as tapes or disk packs from the media librarian as authorized by the file media request forms and mounts or directs a storage operator to mount the media on a peripheral device. The operator then enters commands at the console of the computer that causes the "stack" of jobs, including the subject job, to be processed consecutively but sharing the various system resources asynchronously (not consecutively) as needed to complete the work.

(3) The report containing the requested information comes from the output printer directly connected to the computer or is produced and stored on a tape or disk storage device for off-line printing. The on-line printing may be performed in a spooling mode where the output is saved on tape or disk and printed at a later time in parallel with computer processing of other jobs. The output of the job usually is combined with output of other jobs run at approximately the same time. The printer produces the printed reports on continuous forms separated by one or more pages containing job identification, showing termination of output of one job and the starting of the next. The information consisting of a job number assigned by the computer at input is usually printed in large block letters 3 or 4 inches high that are formed graphically from printing many characters in patterns. This is done for ease of identification, separation, and stacking of the reports. Occasional errors occur in this process where the report for one job is still attached to the report for another job and delivered to the wrong user.

(4) The output report is placed with the job input materials, and all are returned to the user in one of several ways. It may be placed on an open shelf or in an open cubby hole for the user to pick up. It may be delivered to the user's office or an intermediate pickup site by a messenger. Sometimes the material will be placed in a locked cabinet for which the user has the key or lock combination.

c. Backup

Most computer centers have an automatic backup and recovery capability for all jobs, or it is provided at the request of the user (see Section III.A.2.d). If a report or computer-stored data used by a job are inadvertently destroyed, modified, or lost, they can be restored. This is done by saving the tape or disk on which the data were placed for a specified period of time, or on-line computer storage is periodically copied on to an archive backup tape or disk or on request of the user. The tape or disk is stored for a specified period of time in a media library and may be cycled through a remote backup facility, such as a bank vault or warehouse. Commercial services are sometimes used for this backup. The copying is done after each job or possibly each night or on weekends. When the option of backup is given to users, it is frequently not used because of cost or lack of other motivation. Another backup method is to microfilm and archive reports following similar procedures as with tape and disk.

d. Report-Producing Computer Programs

Generalized audit programs are frequently used to produce special reports (see Appendix E). Also report generator utility programs are normally available from within the operating system (see Section VI on Operating Systems). The data selected by naming the files, records and fields may be sorted into various sequences, reordered, and labeled in the required report formats. Data may be coded, formatted, and printed in any form desired; however, if available programs do not meet a specific need, a special program must be developed. Programmers often dislike this type of work and will resist requests for specialized output reports or say that it cannot be done. Reports can be obtained from any computer-readable data, in any format desired, in any desired order within the printer line length, line spacing, and character fonts available according to the printer used. It is only a question of size of effort, programmer skills, and cost.

e. Secure Report Production

Although the following instructions may seem far more elaborate than is practical, anything short of these methods in obtaining and using computer reports as evidence would be attacked by any opposing attorney. The only alternative is to obtain testimony of trustworthy experts to support the less elaborate methods that may be used.

Errors and omissions or malicious intentional acts are possible at each stage in the report-producing process or by nonreal-time program or data modification. Prevention or detection of sufficiently sophisticated intentional acts is often not possible on a practical basis. Therefore, varying degrees of precautions must be taken, and prosecutors must invoke the trust of data processing personnel, depending on potential threats and degree of confidence needed in the integrity and correctness of the report contents.

A moderate level of confidence can be obtained by taking the storage medium (tape or disk) to a different computer center to have its contents printed. Independence should be further ensured by verifying that personnel in the center would have no special interest in the work they would be required to do. Otherwise, the primary concern is to determine that a valid data source has been obtained.

The most elaborate security and integrity can be ensured by following the steps listed below that match the steps presented in Section IV.B.2.b. above for the off-line system mode. This mode is recommended because the on-line system mode is generally less susceptible to high levels of security afforded by direct observation. (There are exceptions where the opposite is true, depending on potential threats in certain situations.)

The following steps also require a trusted computer user and/or one or more observers technically competent in all technical subjects that are identified. A handwritten log should be prepared describing each action taken, naming personnel involved, recording times and places, identifying materials, names, serial numbers of all equipment, computer programs used, and all results.

(1) Preparing the job for submission to the computer system requires obtaining the correct data source medium (tape, disk, cards, or storage device), a test data source in the same type of medium with a human-readable copy of the data, a trusted computer program, a trusted computer operating system, and a trusted computer system. Potential threats include substitution of the data or test sources, Trojan horse modification of the program or operating system, or electronic or mechancial modification of the computer system (see Section I.F. on Computer-Related Crime Methods). A trusted manager of computer operations should be required to directly perform all actions or personally direct his staff. The data storage medium, if of a removable type (tape, disk, cards), should be positively identified as follows:

- Tape: Serial number usually in large block characters affixed by the computer center in which it was first used; tape reel label affixed to the side or flange of the reel identifying the current contents of the tape and usually a date on which the tape was last certified or tested; and an internal label with equivalent content identification and reel number recorded as the tape header or first record on the tape. The latter requires a computer program executed on a computer to determine the content of the label or header.

- Disk: External labels are similar to those for tapes. Internal labels are normally recorded at the beginning of each file of data on the disk or each band or sector.

- Punch cards: Handwritten descriptions of the contents are usually on the top of the deck, on the first card, or on the box containing the cards. The first card or first few cards may have the contents identification punched in them and can be visually read from the printing across the tops of the cards or by decoding the punches in them. Usually one or more cards at the back of the deck will identify the end of the data. Normally, the last few columns of each data card will contain a sequence number and possibly content identification in abbreviated form.

- On-line storage: There is no way to visually identify the data directly. It can only be identified by execution of a computer program that caused the identification to be printed or displayed.

A trusted individual who knows as much as possible about the source of the data should verify the identity of the data and initial the storage medium on the external label. He should also observe the safekeeping of the medium and its usage before, during, and after its use. He should be aware that tape can be spliced, magnetically modified, and wound onto a different reel. A disk could be placed in a different cover or magnetically modified. Punch cards can be replaced, new holes punched, or existing holes covered over. There is no practical way to determine the integrity of data in on-line storage. The only assurance is based on the trustworthiness of all persons with the skills, knowledge, and access to modify the on-line data. This also is the case with removable media, once placed on a computer system storage device.

When the computer program is in a removable medium to be used in the same ways as the data identification described above, a trusted individual should identify it. The copy of the program should be obtained from an independent source where it would be free from tampering by any parties to the crime under investigation. The copy of the operating system and related utility programs should be obtained in the same way. A program and operating system already in on-line computer storage should not be used.

The job set-up process should be observed by the appropriate technical expert. All documents and new data storage media for job input purposes should be logged and initialed by the person supplying and using them.

The integrity of the report-generated program, operating system, and computer system cannot be ensured on a practical basis because they are too large and complex. The capability to prove the correctness of the performance of a program or a computer is a subject for research, and practical capabilities are not expected for several years. [31, 32] Therefore, total trust must be placed in the technologists and vendors who designed, implemented, and maintain the products. The more widely used a product is and the more reputable the vendor, the greater the likelihood of its integrity; nevertheless, it takes only one individual with sufficient skills, knowledge, and access to secretly modify it.

Actions can be taken to partially compensate for this greatest vulnerability of protecting integrity in the production of a report. If the original and computer design engineers programmers, maintenance programmers, and engineers are available, they can be consulted and their trustworthiness evaluated. This may be more practical for the report production program than for the operating system and computer system because these two systems can be so large that hundreds or even thousands of programmers and engineers are involved. It may also be possible to document the care taken in the design and implementation of the products used. Experts and state-of-the-art literature can be used to evaluate and establish reasonable care. Other users of the same products can also aid in determining the trustworthiness of products to be used. Finally, testing of the products can be done as described in the next step described below.

(2) In the computer usage steps, the first task is to reduce the computer system equipment that is on-line and the computer programs in the computer to the practical minimum necessary to produce the report. This may be costly in a large computer system because it requires paying for the entire system rather than sharing it with other users. Choosing a night or weekend period could help reduce cost or reduce the number of users sharing the system. Next, as much residual data and programs as possible should be erased from the system. This is usually too costly for large, secondary storage devices. The operating system should be refreshed in storage from the backup storage medium. The report producing job can then be run using the test data for which the human-readable version is available. The resulting output report can then be checked to assist in ensuring the integrity of the process. The job can then be run with the subject data to produce the desired report. The job could be run a second time to increase confidence by comparing the results.

(3) Independent, trustworty observers with the skills and knowledge to determine correct operations should observe all production steps. Each person involved in producing the report should be identified and should initial the documentation of the materials used

and records produced. Copies of all handwritten logs, journals, and computer-produced documents including the computer console printer log, should be collected.

(4) The information in the computer-produced report should be evaluated for reasonableness. All materials should be carefully preserved. This includes keeping data storage media in proper environments (within heat and humidity constraints). This is required for punch cards as well as magnetic media.

4. Caring for Evidence

Some types of computer-related evidence require special care. Storage environments must be controlled, and physical damage from manual handling must be avoided. Criminal justice agencies normally have evidence storage and archiving facilities, but these environments may not be suited to computer-related evidence and correct handling experience may be lacking. Types of evidence and special needs are described below:

o Magnetic tape and magnetic disk

Storage: 40 degrees F-90 degrees F, 20%-80% RH (80 degrees F Wet Bulb Max.). Unrecorded tape or disk may be stored up to 120 degrees F (90 degrees F Wet Bulb Max.). Storage life for data retention and recovery is 3 years.

Handling: Store, handle, and transport items in hard cover containers. Avoid dropping or squeezing. Always grasp by the hub; touch, bend, or crease no parts of the recording surfaces (the first 5 ft. or leader of tape can be handled and creased). Avoid placing near strong magnetic fields that might be created by a motor or permanent magnet. Affix tags or marks on containers or reel surfaces that do not come in contact with tape or disk drive equipment. Store tape reels vertically in tape storage racks and disk packs on flat wide shelves.

o Punch cards and punch paper tape

Storage: Same as magnetic tape. Storage life indefinite.

Handling: Avoid folding, spinning, or knicking edges. Never use paper clips or rubber bands. Store in metal or cardboard boxes in which they come from manufacturer. Store under mild pressure (in full boxes) to avoid warping. Jog card decks to align them on a job table (on top of card equipment). Wind tape on tape winders only (some tape is accordian folded). Individual cards and pieces of tape can be handled manually, with care not to damage edges or tear. Tagging or marking methods are not critical. Avoid tape that removes paper surfaces or covers punched holes.

o Computer listings

Storage: No restrictions except to avoid strong light to reduce fading. Store on flat surfaces between covers (binders).

Handling: Continuous forms should be bursted into separate pages for ease in reading but not bursted if the continuous form nature of the listing is important to the case. Assure positive page sequence or numbering before bursting to assure correct page sequences. Some printers use special paper that may require special handling for preservation. There are no tagging or marking restrictions.

o Electronic and mechanical components

Storage and handling: Consult the manufacturer or owner for special instructions.

The owners of computer-related evidence may have special problems when the evidence is removed from their possession or custodianship as stated previously. The material may be necessary to continue their legitimate business or other activities. In such cases, the material should be copied in an appropriate, independent, and secure fashion and the copy returned to the rightful owner or user.

5. Privacy and Secrecy of Evidence

Evidence seized in the form of computer media may have data stored that are immaterial to the investigation but that may be confidential to the rightful owner. This could involve the issues of personal privacy, trade secrets, or government secrets. The problem may be solvable by retrieving and copying on another computer medium only the data at issue in the case. However, this frequently is not possible. In such a case, it may be possible to give assurance that the extraneous data will not be revealed and will be stored in a secure manner that is at least as safe as where it was originally found.

Search and seizure right to privacy issues that arise generally can be handled by using the same principles in much the same way as in noncomputer abuse cases. As discussed earlier, the prosecutor should remain alert to these issues; again, taking preventive measures during search and seizure efforts is the best cure.

Nonsearch and seizure right to privacy issues will arise where personal, privileged, or classified information or transactions are involved and reflected on the proffered evidence. Obtaining consent from the individual(s) who are the subjects of the information is sometimes available.

Even where consent is not obtained, sufficient safeguards that are available in most jurisdictions minimize this problem. A hearing outside the presence of the jury or even an 'in camera' hearing may

allow the court to overrule the objection or perhaps excise the specific objectionable portions. With the exercise of such safeguards, the compelling state interest in law enforcement will generally prevail.

C. PROSECUTION

The discussion in this section provides prosecutors with information useful particularly during court proceeedings in computer-related criminal action cases. The discussion introduces technical and legal considerations, as well as practical information on trial tactics.

1. Foundational Problems

Generally, before proffered physical evidence can be admitted into evidence, certain foundational 'preliminary facts' must be proved by the party seeking admission. These preliminary facts are to be contrasted with the facts sought to be proved by the evidence. Quite obviously a principal defense tactic will be to attach admissibility based upon foundational issues, an attack to which the prosecutor is particularly vulnerable.

a. Authentication

Authentication of a written statement generally means the introduction of evidence sufficient to sustain a finding or establishing by other means that the written statement is in fact the writing the proponent of the evidence claims it is. Thus, the prosecutor will need testimony from someone who can verify that the purported maker of the item--namely, the particular computer system that generated the proffered item--is the actual maker. Note that the proponent of a writing satisfies his burden of establishing the preliminary fact of authentication by introducing evidence that is sufficient for a trier of fact to reasonably find that the proffered item is what the proponent claims. Hence, it is critical at this stage not to claim more than simply the output process--i.e., that the proffered item was generated by such-and-such computer at such-and-such place and time, and nothing more.

The prosecutor significantly compounds the authentication problem if an attempt is made at this point to claim that the proffered item reflects a particular configuration or programmed process internally within the computer, or that it reflects particular information fed earlier into the computer. To do so would allow the defense to raise objections based on the authentication of such specific internal configuration or earlier input. These defense objections would be valid because the extended 'claim' infers that the proffered item is merely a copy or secondary evidence of something else. Thus, the 'original' writing--namely, again either the internal configuration or the earlier input--would have to first be authenticated in addition to

authentication of the secondary evidence. These matters would be addressed under the Best Evidence and Hearsay--Business Record Exception rules, and there is certainly no need to double the trouble.

b. Best Evidence Rule

Computers operate by use of electronic signals and magnetic spots not visable to the human eye. Because the law requires that triers of facts be human beings, with human eyes, secondary evidence in the form of computer-generated physical printed matter, purporting to be a copy of the electronic signals will often be essential to successful prosecution.

Thus, the formidable problem of the Best Evidence Rule arises for the prosecutor. Accuracy will need to be foundationally shown, whether in the Federal Rules of Evidence and Rule 255 of the California Evidence Code will deem proffered computer-generated evidence to be an 'original' upon a showing of accuracy, or in a 'copy' jurisdiction where traditional foundational findings are required.

In actuality, the problem is double-barreled. Not only must the court be satisfied that the showing of accuracy has been sufficient to permit the item to be submitted to the trier of fact, but also the trier of fact must independently be persuaded beyond a reasonable doubt on the weight of the evidence that the item is accurate.

The defense will have available plenty of EDP experts who would gladly testify as to the unreliability of computers and the possibility of either hardware or program error at virtually every stage in the computer process, including the output generation components through which the proffered evidence was derived. Expert opinion is so plentiful that, based only on general technological probabilities much less the specific system at issue, the prosecutor's secondary evidence fails the legal standard of accuracy required.

An important caveat to the unsuspecting investigator or prosecutor is not to assume that the documentation of a computer program is an accurate reflection of the actual program in operation at the time of an alleged crime. In most system development projects, the documentation is tyically a last-minute, low-priority effort, often incomplete, and frequently not updated to reflect program changes and modifications made since the program has become operational. Be forewarned that unless the documentation has been recently verified any specific portion of a program should be used cautiously and never offered as eviidence in court unless specifically verified immediately beforehand.

A solution to these problems is to select potential witnesses who not only are experts in the general state of the art, but also have expert familiarity with the computer operations or programming where the

offense occurred. These witnesses should be sought out as early as possible so as to use their knowledge as a resource in determining preventive action when obtaining physical evidence as well as to discuss their testimony. Thus, for example, when seeking a program listing accurately reflecting the actual code, use the 'familiar' witness to secure the program listing from the most accurate source, which might be a machine language 'object code' listing from an on-line program library rather than one stored in some off-line back-up program library stored on tape. This will help to avoid later rulings of inadmissibility of the evidence.

2. Proprietary Rights of Computer Programs

The prosecutor must know the differences among the various forms a computer program takes. It will usually be in source code form, the language in which the programmer wrote it. Assembly code form is the symbolic language that the computer system uses as an intermediate form to translate it into actual machine code that is executed by the computer. It is best to avoid these technical descriptions whenever possible in presenting the evidence. Source code programs often will be executed directly in a computer where the lower, more detailed forms of the programs are immaterial to the execution of the program so long as the internal language translators have an acceptable level of integrity. Therefore, only the souce code version of the program and its input and output need be considered. The integrity of the intermediate forms and processing could be established through expert witnesses.

Not all computer programs are physically labeled as to their ownership. Commercial program packages may have adequate labels in terms of copyright and trade secret law. Sometimes these packages will have secret-coded labels inserted or buried within the program itself -- much like a map maker will put a fictitious name on a map to show ownership. No two nontrivial programs will ever be identical when written by different people even though their function may be identical. Computer programs even in higher level languages will generally be unintelligible to the layman; however, many computer programs are extensively annotated line by line in easy-to-read English that the layman may understand.

Many of these computer programs and computer data are of significant value to their owners. Furthermore, much of the information may be highly sensitive to a business, particularly if it is revealed in open court. Therefore, it is important to understand how computer programs are protected when introduced as evidence (or used in obtaining evidence). The most common and most effective protection is under trade secret laws. Most computer programs that are licensed for use by service bureaus, time-sharing companies, computer vendors, and program vendors are protected as trade secrets and often only their use and not copies are licensed to the customers using these programs.

Demonstration that proprietary information is a trade secret was straightforward in typical environments of the past, and precedents for these traditional areas are well established. However, increasing numbers of assets in the form of data and computer programs that may constitute trade secrets are stored in computers and computer media, and few precedents exist.

A trade secret must be adequately protected. As stated earlier, computer programs are most commonly protected as trade secrets and licensed for use by others in the case of commercial computer programs. The patents on some computer programs have been mainly for processes embodied in electronic circuitry. The U.S. Supreme Court has ruled on three occasions that specific programs were not patentable. Although programs are copyrightable, protection is of minimal value because it protects only the expression of the idea but not the idea itself. Trade secrets may include data that represent secret processes, product specifications, geologic information, business records, or customer lists.

The first step in determining that adequate protection has been applied to qualify data or computer programs as trade secrets is to identify all copies, representations, forms, locations, and custodians of such assets. Most data and programs stored in a computer or computer media will also exist in other forms and locations. In computer-using organizations, disagreement sometimes arises between the computer users, the computer services supplier and the data processing organization over the custody and responsibility for the security of the trade secret. This is usually resolved by finding that each is responsible for the forms of the material in their respective domains. However, the data processing organization may claim that it is unaware of the secret nature of the material among the high volumes of data and programs in its domain. This is especially the case in on-line computer systems where the users control their own data and programs through terminals. In batch-operated systems, it is sometimes not clear at what point custodianship of a job submitted for computer processing or job output passes from one area to the other.

Proof of adequate security for a trade secret consists of the combination of all safeguards and controls of all forms of the secret and the basis on which it may be offered for use by others. In one case (Ward vs California, 1972) of theft of a computer program from the storage of a computer over a telephone line, the following safeguards and controls were accepted as adequate (but may not be adequate under current practices):

- Secret accounting number needed for terminal access.
- Secret site code number needed for terminal access.
- Unlisted telephone number for access to the computer.

- Secret file name in which the computer program was stored.
- Offerings of use of the program by others were restricted to use and not giving copies of the program. (The program was a utility program available only for use in the time-sharing computer.)
- Several inadvertent disclosures of the program were noted but did not constitute loss of trade secret status.
- Data processing employees were aware of the proprietary nature of the program.

This was contested by the defense council who obtained the expert opinion of a witness who stated that it was his practice (although not an industry standard) that any program or data he was able to obtain in any way possible from a commercially available time-sharing service through a terminal was by definition in the public domain if no proprietary notice was given. This was called the Peninsula ethic, because the individual resides on the San Francisco Peninsula. It is not a generally accepted concept, but it shows the lack of concurrence on generally accepted practices. Each expert will have his own ideas about various technical subjects that will differ from others. It is recommended that important concepts to a case stated by an expert be supported in the technical literature or concurrence obtained from at least one other reliable expert.

3. Evidentiary Problems with Computer Records

As a written statement, computer-generated printed evidence offered to prove the truth of the matter asserted must satisfy the Business Record Exception requirements before being admissable as a hearsay exception. Without a reiteration of them, the general purpose of these requirements is to establish reliability and trustworthiness of such written statements. Here again the prosecutor faces the burden of showing computer reliability, an area fraught with complex technological issues. More than ever, the best prosecutorial strategy will be to lead the presumably nontechnical court to focus upon the legal issues rather than getting lost in a technical quagmire. It is important that the prosecutor be prepared to assist the court with prior case law dealing with the issue.

A problem occurs if a computer printout was not generated in the regular course of business, but was printed soley for use in prosecution. If the printout was generated during regular business but at a later time thus reflecting data that were entered or transactions that occurred some time significantly prior to the actual printing, an objection may be raised on the grounds 'made at or near the time of the act' or 'time of preparation.'

The problem is compounded in instances where upon securing the computer facility as the crime site, weeks may be needed with the experts to determine what printouts should be obtained. Short of maintaining guard and forbidding use of the computer facility, an option not ordinarily available, the investigator and prosecutor should be prepared to implement extensive, reliable, and provable labeling and identification procedures. Likewise, complete records tracking storage and custody of all evidence items should be maintained. Careful handling of off-line storage devices including computer tapes and disk packs that may ultimately be used to generate printout evidence is also critical because of their high vulnerability to spoilage or alteration.

A further word of caution is in order. Beware of too much reliance on the testimony of a custodian or other qualified witness to cure singlehandedly all foundational problems that the proffered printout is the one generated at the time of the offense or search, especially where the printout constitutes portions of a computer storage printout or other lengthy or complicated computer display. Again, careful and immediate identification of all potential evidence items is necessary.

After all reasonable precautionary steps have been taken to ensure reliability and trustworthiness, the best response to defense Business Record Exception objections will be to focus upon the law--particularly on the underlying purposes for the law. After the general reliability of the computer system is shown, the court must then be persuaded that within the limitations precipitated by the nature of computer processing, the underlying purposes of the hearsay rule are satisfied.

The issues arising within the last 5 years regarding computer records and the law of evidence fall into three basic categories: (1) the admissibility of computer printouts as evidence; (2) computer printouts as the basis of expert testimony; and (3) discovery matters with regard to computer systems. The first category, admissibility, receives the most attention from the courts and commentators. [See, for example: Note, "Appropriate Foundation Requirements for Admitting Computer Printouts into Evidence," 1977 WASH. U.L.Q. 59 (1977); Note, "A Reconsideration of the Admissibility of Computer-Generated Evidence," 126 U. of Pa. L. Rev. 425 (1977).] Each of these categories is discussed below.

a. Admissibility of Computer Printouts as Evidence

The admissibility of computer printouts as evidence depends on whether the data from which the report is generated were captured and entered into the system in the normal course of business. If so, the data record and reports produced subsequently in the regular course of business or even for trial purposes may be admissible. The following types of reports can be produced from data in computer storage media:

Data	Program	Production
Especially prepared	Special	One time
Especially prepared	Utility	One time
Especially prepared	Production	One time
Production	Utility	One time
Production	Utility	Periodic
Production	Special	One time
Production	Production	Periodic

Definitions of the kinds of data and programs given in the tabulation above are listed below:

- o Especially prepared data: Data are translated from a non-computer storage medium to computer storage medium.
- o Production data: Data are already in the form used for regular and normal production.
- o Utility program: A computer program generally available in a computer system and used for different applications. This includes generalized audit programs.
- o Special program: A computer program especially programmed for one specific purpose. It may also call and use utility programs and operating system functions to perform its job.
- o Production program: A computer program used in a regularly run production job conduct on normal business activities.

Most of the recent decisions regarding the admissibility of computer printouts address the foundational requirements needed to defeat a hearsay objection and show that the computer printouts fit into the business records exception to the hearsay rule. All of the recent decisions surveyed, except one, allowed the admission into evidence of a computer printout. Department of Mental Health v. Beill, 44 Ill. App. 3d 402, 2 Ill. Dec. 655, 357 N.E.2d 875 (1976) In a suit to recover charges for treatment, the court held that the Department had not met the foundational requirements to introduce the computer-generated records.

Criminal Cases -- Courts appear to treat the issue of the admissibility of computer records, both in criminal and civil cases, in a similar manner. In State v. Watson, 192 Neb. 44, 218 N.W.2d 904 (1974), a criminal conviction for writing a check with insufficient funds, the defendant objected to the admission of the bank's computer printout that showed the rejected transactions. The court, in addressing the question of sufficient foundation, noted that the Uniform Business Records as Evidence Act required the custodian to testify regarding the identity of the business record, that the record was made

in the regular course of business, and that it was made contemporaneously. Then the court must determine whether the sources of information and the method and time of preparation justified admission in light of the broad interpretation that should be given to the Uniform Act.

In United States v. Weatherspoon, 581 F.2d 595 (7th Cir. 1978), a conviction for racketeering, mail fraud, and false statements, the defendant enrolled in her beauty school many times the number of VA students allowed. The defendant objected to admission of the government's computer printouts claiming improper foundation. The court, in rejecting the defendant's claim, held that the printouts were computerized compilations of information from enrollment certification forms that had been submitted by the defendant and simply keypunched onto computer tape. Moreover, the testimony of government employees demonstrated the computer system input processes; the accuracy of the printout to 2%; that the computer was tested for internal program errors on a monthly basis; and that the VA made, maintained, and relied on the printouts in the ordinary course of business. Finally, counsel for defendant had been allowed to inquire into the accuracy of the printouts.

Another criminal case, United States v. Scholle, 553 F.2d 1109 (8th Cir. 1977) cert. den. 434 U.S. 940, was a narcotics conviction. At trial, the government introduced a computer printout representing a compilation of information regarding cocaine exhibits that were compiled from the regional laboratory of a district office of the Drug Enforcement Administration. The government also presented the testimony of the doctor who developed the computerized compilation system. The compilation revealed that a particular additive to cocaine, which was very uncommon, appeared in only 2 cases prior to appearing in the cocaine seized and purchased from the defendants. The government was attempting to show, by means of the inference that could be drawn from the compilation evidence, that the defendants were involved in a conspiracy.

In upholding the trial court's exercise of discretion in admitting the compilation, the 8th Circuit noted that the government had provided a proper foundation by demonstrating that the compilations were made routinely and contemporaneously. In addition, the government provided the original source of the computer program and the procedures for input control that ensured accuracy and reliability.

Income tax offense cases often provide situations in which computer records are used as evidence of the tax evasion. In United States v. Fendley, 522 F.2d 181 (5th Cir. 1975), the court rejected the defendant's objection to the introduction of computer printouts on the grounds of accuracy. The court noted that similar printouts had been used in criminal proceedings and that computer printouts are not intrinsically unreliable. Finally, the court noted that the defendant

had an opportunity to inquire into the processes by which the data was input and retrieved from the system, if he had wished to attack the reliability of the printouts.

In United States v. Farris, 517 F.2d 226 (7th Cir. 1975) cert. den. 96 S. Ct. 189, the defendant, convicted of failure to file income tax returns, claimed that the trial court erred in admitting into evidence the output of a computerized data system. The prosecution was not required to show the accuracy of the records, maintained at the National Computer Center. The defendant also claimed a best evidence rule objection, although the director of the Center certified the authenticity of the printout.

The 7th Circuit upheld the admissions of the records under 28 U.S.C. # 1733(b), which allows admission of authorized copies of documents of United States departments or agencies as if they were originals in order to prove by memorandum an act, transaction, or occurrence. At trial, the printout was offered to show that no record of filing a tax return was found after diligent search, and the lack of that record would be evidence showing that the defendant had not filed a tax return.

Civil Cases -- A multitude of different kinds of cases have computer-related evidence issues in the civil arena. In Sears, Roebuck & Co. v. Merla, 142 N.J. Super. 205, 361 A.2d 69 (1976), a collection case, the court upheld the admission of a computer printout alone to prove the debt. The printout showed only the dates of purchase, cost, departments, credit card number, payments made, and balance due, but could not give a description of the goods sold. Sears had destroyed the original invoices of the defendant's purchases so that the only evidence available regarding the defendant's account was the printout. The court held that so long as the proper foundation was laid, a computer printout is admissible on the same basis as any other business record.

In another New Jersey case, which was a mortgage foreclosure action, the court delineated the requirements necessary in laying the foundation for business records. Monarch Federal Savings & Loan Assn. v. Genser, 156 N.J. Super. 107, 383 A.2d 475 (1977). The court held that personal knowledge testimony regarding the information received into the computer is not required, nor is it necessary to have the preparer testify. However, the testimony is required of a custodian or other qualified witness who can testify that the computer records were made in the ordinary course of business, that they were made contemporaneously, what the sources of the information were, and the method and circumstances of preparation.

Many states have enacted the Uniform Business Records as Evidence Act. In construing it, most state courts have reached the conclusion that computer printouts can be business records. One example is Missouri Valley Walnut Co. v. Snider, 569 S.W.2d 324 (Mo. Ct. of App. 1978), a breach of contract case in which the court held that the

computer readouts were admissible under the business records exception to the hearsay rule. Testimony showed that the plaintiff's office manager received information daily from buyers and log inspectors and fed that information into the computer. The computer delivered a printout the following day that was checked for accuracy against the original records.

An interesting twist in this field is the use of computer printouts as summaries prepared specifically for litigation. In United States v. Smyth, 556 F.2d 1179 (5th Cir. 1977), a conviction for conspiracy to defraud and defrauding the United States, the defendant objected to the admission of two sets of FBI computer printouts. The defendant complained that the printouts were simply summaries of records made for purposes of the prosecution and that the headings and explanatory keys were prejudicial. The court allowed the printouts to be introduced, but instructed the jury that they were not evidence but only summaries. The court had all of the underlying documents from which the summaries were made in evidence so that, in conjunction with the jury admonition, there was no prejudicial effect from the summaries.

b. Computer Records as the Basis for Expert Testimony

Two 1976 decisions bear on the questions raised when computer records are used as the basis for expert testimony. In Pearl Brewing Co. v. Joseph Schlitz Brewing Co., 415 F. Supp. 1122 (S.D. Tex. 1976), a complex antitrust suit that also concerns the discussion below regarding discovery matters and computer printouts, the defendant requested discovery of the computer information that was the basis of the expert witness' testimony. The issue before the court was whether the product of computer experts and economic experts working together specially to formulate a highly sophisticated and computerized econometric model for the litigation was discoverable as to the detailed structure of the computer model and alternative methods that the plaintiff had considered but rejected.

The computer model was programmed to test a high volume of data, which simulated market conditions. A damage assessment program also was prepared. Notwithstanding that the plaintiffs had been very cooperative in pretrial discovery, had made available to the defendants printouts of both systems, and had offered to make the trial expert available, the defendant claimed it was inadequate and requested the actual detailed structure of the model. The defendant also wanted to take the depositions of those experts who actually developed and tested the systems, the computer expert - the trial expert's expertise was in economics.

The court held that the detailed structure was discoverable but that the alternative methods were not. It noted that this was not a usual case of business records; rather, the defendant sought expert information prepared specially for trial in a case with exceptional circumstances.

The second case in this same area is Perma Research and Development v. Singer Co., 542 F.2d 111 (2d Cir. 1976) cert. den. 429 U.S. 987, 97 S. Ct. 507. The case was a breach of contract suit in which the plaintiffs claimed breach of the duty to make best efforts. The defendant objected to the use of results of computer simulation as a basis for the plaintiff's expert testimony. The court admitted that the better practice would have been for plaintiffs' counsel to deliver to defense counsel details of the underlying data and theorems used in the simulations before trial so as to avoid discussion of their technical nature during trial. The trial judge was not charged, however, with abuse of discretion for allowing the expert's testimony regarding the results of the computer simulation. The defendant did not show that it had an inadequate basis on which to cross-examine the expert witness.

c. Discovery Matters with Regard to Computer Systems

As was mentioned above, Pearl Brewing Co. v. Joseph Schlitz Brewing Co., 415 F. Supp. 1122 (S.D. Tex. 1976), is one example of the issues raised with regard to discovery and computer systems.

In United States v. Liebert, 519 F.2d 542 (3d Cir. 1975) cert. den. 423 U.S. 985, 96 S. Ct. 392, 46 L Ed. 2d 301 (1975), another discovery case, the issue before the court was whether pretrial discovery may be used to secure extrinsic evidence so as to impeach the reliability of a computer printout, a fundamental element of the prosecution's case. The defendant in this case was charged with failure to file income tax returns. The IRS computers had no record of defendant's filing. The defendant requested that his computer expert have access to the IRS Service Center to analyze and test, particularly for reliability, the IRS data process system. Such request was granted. Then the defendant requested, for discovery purposes, records of the notices sent to persons stating that they had filed no returns or none had been received by the IRS.

The court granted the defendant's request as to a portion of the list of nonfilers. The government refused to comply with the court order so the court dismissed the defendant. On appeal the dismissal was reversed. The appellate court initially noted that pretrial discovery in criminal cases usually is within the court's discretion. It also noted that the admission of printouts in criminal trials was allowed as long as sufficient foundation was laid showing trustworthiness and allowing the opposing party the opportunity to inquire into the accuracy of the computer and the input process. However, the court held that supplying the list that the defendant requested would be unreasonable because of infringement of the right of privacy of those persons on the list. The court noted that the availability of the lists could lead to the defendant in looking for inaccuracies to contacting the persons on the list. The alternative suggestion of the IRS to make available to the defendant all the documents regarding the procedures, operation, and electronic data processing system and the statistical analysis regarding

the capability of the IRS to discover nonfilers and allow their expert witness to be deposed was held sufficient to provide the defendant with an opportunity to question the accuracy of the system.

In United States v. Davey, 543 F.2d 996 (2d Cir. 1976), also a tax evasion prosecution, the issue before the court was whether the IRS may, by summons, compel a taxpayer to produce computer tape that contains part of its financial recordkeeping system. The trial court held that duplicates of the tape at the expense of the IRS would suffice for purposes of the summons. The 2d Circuit overruled the trial court stating that the defendant must supply the original tapes at its own expense. This holding was in accord with the revenue ruling that requires companies with computer-based recordkeeping systems to save their tapes.

Finally, Oppenheimer Fund, Inc. v. Saunders, ---- U.S. ---- 98 S.Ct. 2380, 57 L. Ed. 2d 253, 6 C.L.S.R. 848 (1978), was a class action in which the plaintiffs sought to require the defendant to help in compiling lists so that the plaintiffs could comply with the class action notice requirements. Through depositions of defendant's employees, the plaintiffs determined the class size and discovered that to compile the requested list, someone would have to manually sort through a large volume of paper records, key punch 150,000 to 300,000 computer cards, and create eight new programs at a cost of $16,000.

While the court noted that if the defendant is able to perform the task with less difficulty and expense than the plaintiff, then it is permissible for the district court to order the defendant to perform. However, the defendant should not bear the expense. The court rejected the lower court's holding that because the records were kept on computer tapes it was justifiable to impose a greater burden on the defendant. Although the court realized that some defendants may be tempted to use their computer systems to irretrievably bury information and immunize themselves and their business activity from later scrutiny, it rejected that such was the situation in the present case.

4. Practical Recommendations

a. Expert Witness Testimony

Computer technologists usually have little or no experience as expert witnesses. They must be carefully trained and coached in advance. Do not let a computer expert go out of control: force him to answer in as few words as possible. To achieve this, the questions must be well formulated so as to elicit brief answers. Use the help of experts in formulating the questions as well as the answers.

Computer-generated evidence is only as good as the person who testifies to it. A problem arises when investigators think they can bring in any witness from the victim company to testify that "these are

business records". Witnesses are needed who know what they are talking about and can show that the method of generating the evidence is valid.

b. Technical Presentations

Remember that the most likely image that the judge and jury have of computer technology is what they last read on the front page of the newspaper. This material tends to be highly sensationalized and highly distorted. As with any case, it is wise to leave the jury and the judge with three or four strong points. Make the whole case as basic, simple, and free from computer technology and terminology as possible.

In court, explain only the circumstances and technology necessary to present the case. Avoid bringing computer technology into a case whenever it is possible and does not detract from the strength of the prosecutor's position. It would usually be better to rely on paper records when they exist rather than to introduce computer-generated records.

Do not present the "bits and bytes" of computer logic when decimal numbers, letters of the alphabet and phenomena external to the computer will suffice. In other words, juries do not have to understand telephony to convict an obscene telephone caller. When a case involves computer programs, use the source language forms and ignore compilers,, assemblers and object language forms when not essential to the case. Whenever possible, using analogies to familiar objects is useful in presenting technical concepts; some examples are provided below:

Computer-Related	Analogy
Magnetic tape and tape drives	Cassette and reel-to-reel, audio recordings, and hi-fi equipment
Magnetic disk	Phonograph record
Computer printer and output listing	Printing adding machine, typewriter
Computer terminal with printer	Typewriter
Computer terminal with display	Cable television and home TV games
Computer programs	Food recipes, player piano rolls
Addressable storage	Post office boxes
Terminal access passwords	Combination locks

Computer-Related	Analogy
Data communication	Telegrams or Telex
Real-time and nonreal-time	Selecting food in a cafeteria and ordering from a waiter
Batch and on-line	Using a home dishwasher and using a continuous flow dishwasher in a restaurant
One microsecond (one millionth, 0.000001) compared to one minute	One minute compared to 114 years

As stated earlier, it is important to avoid computer field jargon such as software (computer programs), firmware (computer programs in read-only storage devices), bits (binary digits), IBM cards (punch cards), and bugs (computer program errors). It is important to use the most technically correct, dictionary-defined words and maintain strict differentiation between living persons and computers. Computers are not dumb or smart and do not make errors or commit crimes; only people have these attributes. The point about errors needs further consideration. Computers do not make errors. Errors that result from computer actions stem from human actions such as input errors (garbage in, garbage out), electronic design errors, lack of proper maintenance, or program errors.

Do not personify or anthropomorphize computers in presentations in court. When others do this, use it to demonstrate a lack of technical understanding on their part. Computers should be treated strictly as inanimate objects, machines, subject to the use and manipulation by people. When the judge and jury need an explanation to understand technical issues, use simple diagrams and visual aids extensively.

Visual aids can be used effectively in computer-related crime cases and are often readily available or can be easily prepared. Many of the diagrams and tables in this manual may be useful. Important points to remember are to keep concepts and information as simple as possible and limited to only essential points. The following visual aids are suggested.

Visual Aid	Use
Programmable pocket calculators	Computer program concepts

Visual Aid	Use
Pocket calculators	Illustration of input, output, storage, and number representation
Computer terminal installed in the courtroom with access to a time-sharing service [optional closed circuit television (CCTV) for more effective viewing of terminal]	Demonstration of all computer time-sharing concepts and computer applications
Charts	Data flow, computer concepts, programming concepts
Photo blowups	Evidence detail, computer equipment detail
Tapes, disks, punch cards	Examples of computer media
Computer vendor-provided motion picture films	Presentation of most computer concepts

When large volumes of writing are to be presented in court, the "best evidence rule" may be inapplicable. Therefore, California prosecutors should refer to code number 1509 of the California Evidence Code regarding "compilation evidence." One recommendation for cases with a large volume of evidence is to assemble a single exhibit book containing all documents, send copies to the defense and to the judge, and introduce it as a single exhibit in court. This saves time in court. Prepare a record of exhibits, the counts each is connected with, and the names of the witnesses who are to testify as to each item.

c. Immunity

Some kind of immunity is necessary in complicated computer cases. Co-conspirators are needed as witnesses because the proof problems are difficult without them. If they are granted immunity, however, the jurors tend to be lenient with the defendant; for that reason, some prosecutors try to avoid formal immunity. A prosecutor could tell the individual that he is likely to be prosecuted, yet indicate that his testimony would be a mitigating factor. Another point is that juries usually do not sympathize with the victim that is a large business or government agency that could "afford the loss."

d. Judges

Always determine the judge's degree of knowledge of computer technology. Judges vary widely in their knowledge of computer technology and in their attitudes concerning the knowledge they think they have of computer technology. On the basis that a little knowledge can be a dangerous thing, a judge who has had a brief course on computer technology may be more difficult to deal with than a judge who has had no briefings on computer technology. Brief courses on computer technology make the technology too simple in too many respects. The effort required to develop computer programs, the likelihood of adequate integrity of computer programs, and the complexity of the programs can often be made deceivingly simple.

SECTION V COMPUTER-RELATED CRIME LAW

The purpose of this section is to aid prosecutors by identifying and summarizing state and federal statutes and proposed legislation applicable to computer-related crime. Prosecutors have stated that statutes have been found to prosecute all cases of computer-related crime coming to their attention. However, the laws were not written in anticipation of high technology crime, and in some cases prosecution has been difficult and obtuse.

The need for laws directly applicable to computer-related crime has recently been recognized and is currently under development. Therefore, new laws are being adopted at a rapid rate making it difficult for any discussion to be completely timely. This section is expected to be partially obsolete by the time it is published, but the urgent need for a summary of applicable law justified the writing. Updates of this section will be needed soon after publication.

A. STATE PENAL LAWS

1. Computer-Related Crime Laws of Selected States

As of this date, crime legislation specific to computers has been enacted in 6 states: Florida, Colorado, Rhode Island, Michigan, New Mexico, and Arizona. The text of these bills is in Appendix B. A summary and short analysis of 3 of these laws follows.

a. Florida Computer Crime Act [Fla. Stat. Ann. #815.01 et seq. (West Supp. 1979)]

Summary -- The Act proscribes several offenses. These are offenses against intellectual property including data and programs, offenses against computer equipment and supplies, and offenses against computer users. Intellectual property includes programs and data existing within or without a computer (system or network). The offenses against intellectual property are willfully and without authority: (1) modifying data, programs, or supporting documentation; (2) destroying data, programs, or supporting documentation; (3) disclosing or taking data, programs, or supporting documentation that are trade secrets or confidential. Such acts are felonies of the third degree unless the offense is committed for the purpose of devising or executing a scheme or artifice to defraud or obtain any property; in which case, the crime is a felony in the second degree.

Offenses to computer equipment and supplies (the terms are not further defined by the law) include willfully, knowingly and without authorization modifying such equipment or supplies. That crime is a misdemeanor of the first degree unless the offense is for the purpose of devising a scheme or artifice to defraud or to obtain any property; in

which case, the offense is a felony of the third degree. The offense of willfully, knowingly, and without authorization destroying, taking, injuring or damaging a computer (system, network) or equipment or supplies used or intended to be used in a computer (system, network) is a misdemeanor of the first degree if the damage is $200 or less and a felony of the third degree if the damage is between $200 and $1,000. If the damage is $1,000 or more or if there is an interruption or impairment of governmental operation or public communication, transportation, or supply of water, gas, or other public service, the felony is of the second degree.

Offenses to computer users include willfully, knowingly, and without authorization accessing or causing to be accessed a computer (system, network) or willfully, knowingly, and without authorization causing the denial of computer system services to an authorized user of the services which are owned by, under contract to, or operated for, on behalf of in whole or in part, or in connection with another. The offense is a felony of the third degree unless it is committed for the purpose of devising or executing a scheme or artifice to defraud or obtain property. In that event the offense is a felony of the second degree.

Finally, the law states that it is not intended to preclude the applicability of other Florida criminal law.

Analysis -- The law covers acts or theft of and damage to computer equipment, supplies, programs, and data. It covers willful unauthorized access to computers (systems, networks) and denial of services to users. The offenses to intellectual property (programs and data) apply whether or not the property is stored inside a computer: that is, the law applies to programs and data contained in listings, tapes, disks, cards, and other off-line and on-line media of expression. The law does not require the media of storage to be a "thing", and consequently, electronic impulses should be includable. Such inclusion will ease the finding of a taking when a program is taken, modified, or destroyed over telephone lines, as in the Ward [Ward 1972] and Seidlitz [Seidlitz 1978] cases.

Because unauthorized is not defined by the law and because access is defined so poorly, the prohibition against theft of computer services, such as computer time is not clearcut. Florida appears to have no specific theft or services statute, and the property theft statute [Fla. Stat. Ann. # 811.021(1)(a) (Supp. 1975)], "anything of value," would have to be interpreted to include services. Because applicability of both the new law and the prior property theft law is unclear, obtaining a conviction for theft of services such as computer time may remain difficult in Florida.

A particular advantage of the Florida law is that computer programs or data stored other than in a computer qualify as intellectual property within the meaning of the statute. This will aid in the prosecution of

thefts, disclosures, alterations, and destructions that do occur to computer products but were not covered by prior law.

b. Colorado Computer Crime Law [C.R.S. #18-5.5-101 (1973, 1978 Repl. Vol.)]

Summary -- The Act proscribes the knowing use of a computer for fraudulent purposes, the assault or malicious destruction of a computer, and the unauthorized use or alteration of a computer or its "software" or data. Penalties relate to the value of the item stolen: under $200 of loss or damage is a misdemeanor punishable by a fine and jail sentence up to 12 months; loss or damage over $200 is a felony punishable by a fine and jail sentence up to 40 years.

Offenses that are fraud-related are those in which knowing use (use is defined to mean to instruct, communicate with, store data in, retrieve data from, or otherwise make use of a computer, computer system, or computer network) is made of a computer (system, network) for the purpose of devising or executing a scheme to defraud; obtaining money, property, or services by false pretenses; or committing theft.

The other form of computer crime is the knowing and unauthorized use, alteration, damage, or destruction of a computer (system, network).

The graduated classification of offense and associated penalties relate to the dollar value of the loss. Currently, these are: under $50 is a Class 3 misdemeanor, $50 to $199 is a Class 2 misdemeanor; $200-$9,999 is a Class 4 felony, and $10,000 and above is a Class 3 felony. (The Class 3 felony also includes offenses, such as child abuse, that result in serious bodily injury).

Analysis -- This legislation is modeled on the Florida law. However, it is narrower in coverage in that data and programs must be "contained in such computer..." to be the subject of the Colorado law damage, alteration, or destruction provisions. Further, it appears that theft or fraud involving property (which includes information and electronically produced data and "software") must be accomplished by use of a computer to fall within the prescriptions of the law.

Further, there is no sanction for denial of computer services unless such denial is part of a scheme to defraud.

The law is in response to the inadequacies of existing law in that it did not contemplate computer abuse and could not be stretched to accommodate the new forms of wrongful activity. In particular, in a case decided by the Colorado Supreme Court sitting en banc on March 19, 1979, the court held that the unauthorized reading and later transcription of a medical record without a taking of the physical record did not constitute a theft because the medical information was not a "thing of value" within the meaning of the theft statute. (People v. Home Insurance Co., No. 27984.)

The law's definitions--the weakpoint in most existing and pending computer crime legislation--are somewhat more precise than other attempts in this area but there are still problems with defining "software" and "hardware" in the dynamic technological melieu.

c. Arizona Computer Fraud [Ariz. Rev. Stat. Ann. #13-2301 and #13.2316 (Swest 1978)]

Summary -- The Arizona statute in its general criminal fraud provisions defines in # 13-2301 for the purposes of # 13-2316 various terms with regard to computers--e.g., "access, computer, computer network, computer program, computer software, computer system, financial instrument, property, and services." Section 2316 provides for the offense of computer fraud. This section provides that a person commits computer fraud by accessing, altering, damaging, or destroying without authorization any computer, computer system, computer network with the intent to devise or execute any scheme or artifice to defraud, deceive, or control property or services by means of false or fraudulent pretenses, representations, or promises.

Computer fraud in the first degree, punishable by up to 5 years in prison, is committed when a person accesses, alters, damages, or destroys a computer (system, network) without authorization and with intent to devise or execute a scheme to defraud or to control property or services by false or fraudulent pretenses.

Computer fraud in the second degree, punishable by up to 1-1/2 years in prison, is committed by an "unauthorized, intentional access, alteration, damage, or destruction of a computer (system, network) or any software, program, or data contained therein."

Analysis -- This law, which was passed at about the same time as the Florida law but independent thereof, is somewhat similar in that it covers hardware, programs, and services. Note that "software, programs, and data" must be contained in the computer before such "data and programs" are covered by the law. Otherwise, other Arizona law applied to intellectual or intangible property will have to be applied.

The legislature has coined a definition of "software" that encompasses a related group of programs, procedures, and documentation associated with the operation of a computer system. It is of utmost importance when applying any computer crime law to read carefully the definitions therein because they will differ from each other and unfortunately from common usage in the computer field as well.

2. Proposed Computer-Related Crime Bills

As of this date, thirteen computer-related crime bills have been introduced in 12 different states. These bills are as follows:

State	Bill Number	Definition of Bill
California	S.66	Prohibits direct or indirect use of a computer, computer system, or network for criminal purposes.
Hawaii	S.504	Prohibits use of computers for criminal purposes.
Illinois	H.1207	Makes it illegal to alter computer programs without consent of owner.
Maryland	H.497	Prohibits fraud by use of a computer and establishes penalties.
Maryland	S.908	Prohibits fraud by use of a computer.
Michigan	H.B.4112	Prohibits computer fraud.
Minnesota	S.F.1033	Prohibits data and data processing equipment related fraud and destruction.
Missouri	S.230	Relates to computer systems, networks, equipment and supplies with penalty provisions.
New Mexico	S.8	Makes misuse of computers a crime.
North Carolina	S.397	Makes computer-related crime a felony.
Tennessee	H.114	Makes unauthorized use of computer equipment a criminal offense.
Tennessee	S.172	Same as H.114.
Utah	H.183	Prohibits computer fraud.

Copies of these bills are in Appendix C. Note that the Ribicoff Federal Bill, S.240 in Appendix A, would apply to many computer systems located throughout the several states.

B. OTHER STATE AUTHORITY BEARING ON COMPUTER-RELATED CRIME

1. Automatic Banking Devices

Kentucky has a recent statute, Ky. Rev. Stat. # 434. 685 (Supp. 1978), that proscribes the misuse of electrical information with regard to automatic banking devices and EFTs. Note that a new federal law, Title XX of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), also proscribes EFT crimes.

2. Credit Card Crime

Many computer-related crimes consist of or include unauthorized access of a computer system to obtain, alter, damage, or destroy programs, data, or services, such as computer usage. Apart from theft of computer programs (which is discussed separately below), it may be possible to charge a perpetrator with credit card crime, forgery, theft of property, services, or a thing of value under charges of false pretenses and burglary. Most jurisdictions now have credit card abuse laws, e.g.,

ALA. CODE Tit. 13 # 4-32 4-41 (1977)

ALASKA STAT. # 11.46 2285 (fraudulent use of credit card), # 11.46.290 (obtaining a credit card by fraudulent means)

ARK. STAT. ANN. # 41-2308 (1977)

GA. CODE ANN. # 26-1705 to # 26-1705.10

HAW. REV. STAT. # 851-10

ILL. ANN. STAT. ch. 121 1/2, # 60 ch. 121 1/2, # 601 et seq. (Supp. 1978)

IND. CODE ANN. # 35-43-51 to 35-43-55 (1979)

IOWA CODE ANN. # 715.1 to 715.6 (West Supp. 1978)

KAN. CRIM. CODE & CODE OF CRIM. PROC. # 16.841-16.844 (1974)

KY. REV. STAT. # 434.550-434.730 (Supp. 1978)

LA. REV. STAT. ANN. # 14.67 (1974)

ME. Rev. Stat. Tit. 17-A # 905 (Supp. 1978)

MD. CRIM. LAW. CODE ANN. # 145 (Supp. 1978)

MINN. STAT. ANN. # 609.52 (West Supp. 1979)

MONT. REV. CODE ANN. 94-6-307 (Supp. 1974)

NEV. REV. STAT. # 205.610-205.810 (1977)

N.M. STAT. ANN. # 30.16.24-30.16.38 (1978)

N.C. GEN. STAT. # 14-113.8-.17 (Supp. 1977)

OHIO REV. CODE ANN. # 2913.21 (Supp. 1978)

S.C. CODE # 16-13-270 & 280 (1976)

R.I. GEN. LAWS # 11-49-12 to 13 (Supp. 1978)

S.D. COMPILED LAWS ANN. # 22-30 A-8.1 (Supp. 1977)

UTAH CODE ANN. # 76-6-506.3 (1978)

WIS. STAT. ANN. # 943.41 (West Supp. 1979)

WASH. REV. CODE ANN. # 9A.56 (1977)

Whether these may be used to prosecute will depend on the fact pattern and the statutory language. For example, in some jurisdictions, uttering a fictitious account number is enough to trigger the law. See, e.g., Del. Code Ann. Title 11, # 904 (1975) ("credit card" includes writings, numbers, or other evidences of undertaking to pay for property). In other jurisdictions, the actor must actually "utter a fictitious card," thus, an account number system where no credit cards are actually issued probably would not trigger the statute. See, e.g., Va. Code Ann. # 18.1-125.2(2) (Sup. 1974) ("credit card" means instrument or device).

3. Theft by Deceit

With respect to theft by deceit in a recent Missouri Case, State v. Hamma, 569 S.W.2d 289 (Mo. Ct. App. 1978) decided before the passage of the Financial Institutions Regulatory Act (FIRA), the defendant was accused of stealing by deceit. On appeal he contended that the information did not state conduct constituting the crime charged. The defendant was accused of intentionally stealing $800 by deceit by obtaining someone else's automatic teller bank card and secret identification number and taking money out of the machine at $50 each withdrawal. Defendant contended that he made no representation let alone a fraudulent representation and argued that the offense required a verbal misrepresentation to the party defrauded. The court rejected that argument stating that a misrepresentation could consist of any act, word, symbol, or token calculated and intended to deceive. The court held that the deceit may be made either expressly or by implication.

Moreover, the court held that the fraudulent manipulation of an automatic teller is analogous to the use of stolen credit cards, and it cited an earlier D.C. case, Hymes v. U.S., 260 A.2d 679 (D.C. App. 1970), as precedent.

In a recent Virginia case, Lund v. Commonwealth, 217 Va. 688, 232 S.E.2d 745 (1977), the defendant was charged with theft of keys, computer cards, computer printouts from a university and using, without authority, computer operation time and services with intent to defraud. The defendant was a graduate student in statistics and a Ph.D. candidate whose dissertation required the use of the computer. He used over $26,000 worth of computer time. The defendant contended that the conviction of grand larceny was faulty because there was no evidence that the articles stolen--e.g., keys, cards, and printouts--were worth over $100 and that computer time and services were not subjects of larceny. The court agreed, holding that the phrase "goods and chattels" could not be interpreted to include computer time and services in view of the rule that criminal statutes must be strictly construed. Moreover, the court held that the unauthorized use of the computer was not the subject of larceny because nowhere in the criminal code section was the word "use" used. The court cited a 1927 case that held that the use of the machinery in spinning facilities did not constitute larceny.

Finally, the Commonwealth contended that although the printouts had no market value, they should be valued by the cost of labor and materials to produce them. The court rejected that argument and also stated that if there was no market value, the only value that could be used was actual value and in this case the only actual value was to the defendant. The court compared Hancock v. State, 402 S.W.2d 906 (Tex. Crim. App. 1966) (theft of a computer tape containing a valuable program), where the criminal statute was sufficient upon which to base a conviction and the program stolen had a monetary value.

4. Forgery

To obtain access to another's computer system, the actor will need to discover and use the owner's confidential entry code to the system and his account number. The use of this false entry code for the purpose of defrauding or injuring any party may be forgery. Although jurisdictions that have retained the common law requirements of a signature and document would not be applicable, a number of jurisdictions--e.g., California, New York, the District of Columbia, Delaware, Texas and Pennsylvania--have expanded the common law scope of the crime so that any making, altering, executing, completing, or authenticating of any seal, signature, writing, or symbol of right, privilege, or identification that may defraud or injure another is forgery.

The California Penal Code, # 470 (West 1970), provides, inter alia, that anyone who "...counterfeits or forges the seal or handwriting of another..." is guilty of forgery. The central question is whether the entry code is either a seal or a signature. It is possible to analogize the entry code to the signature on a check (itself a form of computerized draft which uses OCR) or the authenticating seal of a notary or official. Moreover, in the only reported case to construe this clause, People v. Burkett, 271 Cal. App. 2d 130, 74 Cal. Rptr. 692 (1969), the court held that "seal or handwriting" was a "catch-all," broad enough to include a photocopy of a reproduction of a seal and a facsimile signature. The defendant had used photocopies of dollar bills in dollar bill changers, 271 Cal. App. 2d at 134, 74 Cal. Rptr. at 694.

The New York forgery statute, N.Y. Penal Law # 170.00 et seq. (McKinney 1967), is a statutory, not common law, offense and covers any false making of private writings that might operate to the prejudice of another.

The remaining three states, Delaware, Texas and Pennsylvania, have similar forgery statutes, apparently patterned after the Model Penal Code. Each includes as protected writings any symbols of "value, right, privilege or identification." Pa. Stat. Ann. Title 18, # 4101(b) (1973); Del. Code Ann. Title 11, # 863 (1975); Tex. Stat. Ann., Penal Code # 32.21(a)(2)(c) (1974). The offense is a felony in Texas and Delaware and a misdemeanor of the first degree in Pennsylvania.

Thus, in at least six jurisdictions, it is quite probable that the use of a false entry code, a symbol of right, privilege, and identification that prints out on any machine and is used to defraud or injure is forgery. As noted in conjunction with credit card abuse, the prosecutor will need to prove a fraud or injury, actual or intended, to trigger the statute. Even though it seems logical that any pecuniary loss should be sufficient, the prosecutor may want to charge at least one of the various theft charges applicable in that proof of value then would not be at issue.

5. Obliteration or Bugging of Programs

Obliteration or bugging of programs is a form of computer abuse that can be broadly characterized as criminal or malicious mischief. Whereas most jurisdictions have criminal mischief statutes of one type or another that proscribe physical damage to another's personal property, some also have "interference with use" statutes that make it a crime to tamper or interfere with another's property so that he suffers loss.

a. Physical Damage

So long as the prosecutor successfully characterizes the damage, he should have no difficulty where the outward appearance of the disk or tape is unchanged. The problem of successful characterization in

California should be minimized by People v. Dolbeer, 214 Cal. App. 2d 619, 29 Cal. Rptr. 573 (1963). California's malicious mischief statute, Cal. Penal Code # 394 (West 1970), provides that any malicious injury or destruction of personal property of another is a misdemeanor.

Five other jurisdictions--Massachusetts, Mass. Gen. Laws Ch. 266, # 127 (1968); Delaware, Del. Code Ann. Title 11, # 811(a)(1) (1975); the District of Columbia, D.C. Code # 22-403 (1967); Florida, Fla. Stat. Ann. # 806.13 (Supp. 1976); and Virginia, Va. Code Ann. # 18.1-172 (Supp. 1974)--have malicious or criminal mischief statutes virtually identical to that of California. Penalties generally vary according to the amount of damage (except in Virginia), and large amounts of damage may give rise to felony charges in Delaware and Florida and felony-level punishment in Massachusetts and the District of Columbia.

Unlike the jurisdictions discussed above (which deal with tangible or personal property), New York's criminal mischief statutes use the general word "property," N.Y. Penal Law # 145.00 et seq. (McKinney 1967). But property subject to theft, N.Y. Penal Law # 155.00(1) defines property subject to theft as "money, personal property...thing in action, evidence of debt or contract, or any article, substance or thing of value." Property for purposes of the criminal mischief and tampering statutes means tangible property. See, R. Denzer and P. McQuillan, Practice Commentary # 145.00, N.Y. Penal Law (McKinney 1967) citing Polychrome Corp. v. Lithotech Corp. 4 App. Div. 968, 168 N.Y.S.2d 346 (1957) (predecessor to current criminal mischief statute not intended to apply to violations of incorporeal rights). Thus, although the statute differs slightly from the California statute, the characterization problem is the same.

The New Jersey malicious mischief statutes, N.J. Stat. Ann. ## 2A; 122-1 and 17036 (1969), use differing descriptions of the thing protected, whereas the former refers to personal property, the latter refers to property. In State v. Shultz, 41 N.J.L.J. 176, 177 (1918), a lower court emphasized that "in order that the offense of malicious mischief may be perpetrated, it is necessary that there be injury to property; but...it is not necessary that the property be entirely destroyed." The operation of the New Jersey malicious mischief statute is unique among all the jurisdictions surveyed. When any malicious mischief occurs, the prosecutor charges a misdemeanor. N.J. Stat. Ann. # 2A; 122-1 (1969). But if the prosecutor fails to prove that the value of the property damaged was more than $200, the defendant cannot be convicted of a misdemeanor, but can only be adjudged a disorderly person, punishable by up to six months in jail and/or a fine up to $500. State v. Tonnisen, 92 N.J. Super. 452, 224 A.2d 21 (1966).

Pennsylvania's criminal mischief statute is generally inapplicable because Pa. Stat. Ann. Title 18 # 3304(a) (1) and (2) are limited to destruction by dangerous means or so as to cause danger to person or property. However, Subsection (a)(3) appears to incorporate theft by false pretenses and extortion into criminal mischief, perhaps as a

smaller included offense of theft. As such, it would be applicable where any loss was caused and the actor used deception to accomplish the mischief. Criminal mischief may be a summary offense, misdemeanor, or felony depending on the amount of loss. Pa. Stat. Ann. Title 18, # 3304(6).

Two Texas statutes may be relevant in the case of damage to programs. The Texas criminal mischief statute, Tex. Stat. Ann., Penal Code # 28.03 (1947), Subsection (a)(1), provides that damage or destruction of tangible property of another is an offense. That is not unusual. However, Texas law also proscribes any alteration or destruction of a writing with intent to defraud. While the law resembles the forgery statute in its scope, it extends to any alteration irrespective of what the writing purports to be. See, Tex. Stat. Ann., Penal Code # 32.47 (1974). Thus, so long as the damage is to printed programs, this provision would be applicable.

The Illinois criminal mischief statute, Ill. Ann. Stat. Ch. 38, 21-1 (Smith-Hurd 1970), specifically proscribes damage to articles representing trade secrets. The statute provides that knowing damage to property of another is an offense. Property is defined as "anything of value," including articles representing secret scientific information, and this definition applies to all offenses against property. The offense is punishable by up to 5 years in prison and a fine up to $500 if the value of the program damaged exceeds $150.

b. Interference with Use

Aside from the Pennsylvania statute, which might be used in a tampering situation but does not specifically refer to interference with use as a crime, Pa. Stat. Ann. Title 18, # 3304(a)(3) (1973), statutes in four other jurisdictions make criminal tampering a punishable offense.

Under the general rubric of criminal trespass, the California Penal Code, # 602(j), provides that entry of lands with intent to interfere with any lawful business is a misdemeanor. New York has a broad array of antitampering statutes. N.Y. Penal Law # 145.20 (criminal tampering in the first degree, a Class D felony) would be applicable to any tampering with a publicly-owned computer operation. That statute contains a broad provision, # 145.15(1) (criminal tampering in the second degree, a Class B misdemeanor) that applies to any tampering with any property which causes substantial inconvenience. It is also a Class B misdemeanor to create a risk of substantial damage to property whether or not such damage occurs. Substantial damage is defined as damage in excess of $250.

Texas has an analogue to the New York antitampering statute. Tex. Stat. Ann., Penal Code 6 28.03(a)(2) (1974). A violation is a Class C misdemeanor if the tampering caused substantial inconvenience of no ascertainable monetary amount, and a misdemeanor or felony if the amount

of loss is calculable. The Virginia statute, Va. Code Ann. # 18.1-183 (Supp. 1974), is similar to the California criminal trespass statute discussed above but, unlike the California law, specifically extends its scope to any interference "with the rights of the owner, user, or the occupant thereof..." As in California, the offense is a misdemeanor.

6. Misappropriation of Programs

Computer abuse in this category of misappropriation of programs may take several forms: (a) unauthorized or fraudulent access to programs by an unprivileged user of a facility or by a privileged user of the facility who has no authorized access to the programs; (b) unauthorized or fraudulent disclosure of proprietary programs by an employee, former employee, or contract program developer. The leading reported case of this category is Hancock v. State, 1 CLSR 562, 402 S.W.2d 906 (Tex. Crim. App. 1966). In Hancock, the defendant-employee offered a listing of 59 programs for sale to a person he thought was an agent of one of his employer's clients.

The scope of state criminal laws protecting programs is often determined by whether the programs are included with property otherwise subject to protection. An initial question is whether unpatented and uncopyrighted programs may be protected by criminal trade secret laws. In states that have no trade secret laws, or where dual charges of larceny and theft of trade secrets may be maintained, [see e.g., Ward v. Superior Court, 3 CLSR 206 (Memorandum opinion 51629, 1972)], the prosecutor must determine whether programs are property subject to larceny. In states that have no criminal trade secret laws, the prosecutor must often look to general "offenses against property" statutes to punish the type of computer abuses noted above. Such general statutes are almost the exclusive remedy in all states for obliteration or bugging.

Three preliminary points should be examined. (1) Computer programs, a form of intangible intellectual property, should be protected by state criminal laws. For excellent discussions of the inadequacy of civil remedies, see Comment, Industrial Espionage: Piracy of Secret Scientific and Technical Information, 14 U.C.L.A. L. Rev. 911, 927 (1967) and Comment, Protection of Trade Secrets in Florida, 24 U. Fla. L. Rev. 721 (1972). First, without protection, a program developer has little incentive for creating and investing. Second, it is only just that a laborer enjoy the fruit of his labors. Third, the criminal law must prevent misappropriation, misuse, and distortion of proprietary programs. See Galbi, Copyright and Unfair Competition, 3 CLS # 4-3, Art. 1, and Bender, Trade Secret Protection of Software, 38 Geo. Wash. L. Rev. 51629 (1972).

(2) With the exception of trade secrets laws, almost all state offenses against property statutes antedate the advent of computers. Definitions and case interpretations may make prosecution for abuse of an intangible difficult. For instance, abuse of programs by copying or unauthorized communication may be seen as a mere disclosure of an idea. Malicious mischief may be deemed only a re-arrangement of magnetic discontinuities with no requisite damage or destruction to the tangible property carrying the programs.

(3) Whether a particular abuse may be successfully prosecuted under larceny or malicious mischief statutes may turn on the skill of the prosecuting attorney in framing the charge where a person has misappropriated programs contained on a magnetic tape or on a printout. Hancock, 1 CLSR 562, 402 S.W.2d 906 (Tex. Crim. App. 1966), shows that so long as the value of the intangible intellectual property is added to the value of the tape or paper (a reasonable addition in that it is doubtful that the tape or paper would have been stolen but for the program value) an indictment or information charging grand larceny should be upheld against a motion to dismiss. A closer question might concern the actor who was ignorant of the program's existence but set out to steal bulk paper or computer tapes per se. The general rule appears to be that the prosecution is not required to prove knowledge of value by the thief [see e.g., People v. Earle, 222 Cal. App. 2d 476, 35 Cal. Rptr. 265 (1963)], and that the market value is fair market value to disinterested buyers and sellers. See also People v. Dolbeer, 214 Cal. App. 2d 619, 623, 29 Cal. Rptr. 573, 575 (1963) (the value of telephone company customer lists is determined by "effort...efficiency...and...secrecy...," not the paper alone).

Where an actor obliterates or bugs programs by altering the magnetic tape or printout, the prosecutor must urge that the "property" which was "injured" under the common form of malicious mischief statutes was the tangible tape or paper. What gives the paper or tape value is the program, see Hancock v. Decker, 1 CLSR 858, 379 F.2d 552 (5th Cir. 1967); when one obliterates the program he obviously injures the tape by rendering it unfit for its purpose. Just as in larceny prosecutions, the prosecutor must be careful to characterize the conduct so as to bring it within the statutory proscription, for example, (1) the thing injured was a tangible tape and (2) the injury was the obliteration of the program. This method of characterization was suggested by John Kaplan, former prosecuting attorney, currently Professor of Law, Stanford School of Law.

Only in two instances will the abuse of programs probably be unprotected under common larceny statutes. First, where the actor copies a program on his own paper or tape and asports the copies but leaves the originals, he has not committed common law larceny as interpreted in most jurisdictions. But see Ward v. Superior Court, 3 CLSR 206 (Memorandum opinion 51629, 1972, sustaining a grand theft charge under a similar fact pattern). The result in Ward is logical, since one who asports a copy of a program steals both value and control

of the property. But the fact that so many states have found a need specifically to proscribe copying a trade secret, Cal. Penal Code # 499c(b)(3)-(4) (West 1970), demonstrates how resistant most courts have been to accepting value or control theories as equivalent to the more traditional "permanent deprivation" thoery of larcenous intent.

Second, where one takes knowledge or electronic signals, he has probably not committee larceny within common law statutes. In Ward v. Superior Court [Ward 1972], Judge Sparrow stated that electronic impulses "...are not tangible and hence do not constitute an 'article' capable of being stolen within California's trade secrets law." 3 CLSR 206, 208 (Memorandum opinion 51629, 1972). This opinion may well represent the popular perception of electronic impulses as outside the scope of property protected by statute. As to theft of knowledge, theses that ideas may not be stolen seems to preclude prosecution of one who develops a program and uses the knowledge gained thereby for a competitor or for himself. But see Tex. Stat. Anns., Penal Code # 31.05(b)(3) (1974) (any communication or transmission of a trade secret without consent is a felony of the third degree).

When an actor misappropriates computer programs stored in a computer, he may run afoul of several other types of laws. First, the state may denominate misappropriation of trade secrets as a separate and distinct offense. Second, notwithstanding trade secrets laws, the actor may be guilty of larceny; as a corollary, and recipient of the program, other than the actor, would be receiving stolen goods. Third, the offender may have committed one or more of the crimes set forth above.

7. Trade Secrets

The Restatement test of a trade secret is that the process, item, etc., be used in the trade or business, be kept secret, and give the owner a competitive advantage over those who do not know it. Trade secret misappropriation statutes are enormously useful in cases of program theft but should be analyzed carefully to make sure the technical requisites have been met. (For example, in Ward [1972], the judge held that the transference of electronic impulses did not constitute a taking.)

Larceny statutes are relevant in three different contexts related to trade secrets. First, in states that have misappropriation of trade secrets as a separate and distinct offense, a dual charge of larceny and theft (or abuse) of trade secrets may arise from the same act. Cf. Ward v. Superior Court, 3 CLSR 206 (Memorandum opinion 51629, 1972). This does not mean, however, that double punishment may be meted out when an actor engages in a single, indivisible transaction that may encompass several crimes. Only the single, heaviest punishment of all the crimes may be imposed. The critical question is what constitutes a single indivisible transaction. Second, where theft of trade secrets is subsumed into the general larceny statute, the burden of the prosecutor to prove trade secrets as property subject to larceny is eliminated.

Third, even where trade secrets have not been statutorily included as property subject to larceny, the prosecutor may be able to prove that the secret is a "thing of value."

The New York larceny statute, N.Y. Penal Law # 155.30 (McKinney Supp. 1974), is an excellent example of how a jurisdiction may include trade secrets, " secret scientific material," in its larceny statute. Both stealing and copying are separate offenses, each a Class E felony. If the trade secret has a readily ascertainable value (market or replacement value, see # 155.20) in excess of $1,500, the prosecutor may desire to waive prosecution under # 155.30 and instead charge second degree grand larceny, # 155.35, a Class D felony punishable by 1 to 7 years in prison and a discretionary fine similar to that for Class E felonies.

Unlike New York law, the California theft statute, Cal. Penal Code # 48a (West 1970), nowhere specifically includes trade secrets as property subject to theft. Whereas the trade secret provision, Cal. Penal Code # 499c (West 1970), is probably the exclusive sanction for copying a trade secret without asportation, Cf. Bender, Trade Secret Protection of Software, the Ward [1972] case indicates that a dual charge of theft and theft of trade secrets is maintainable where an article representing a trade secret, or a copy thereof, is asported.

Although New York is the only state which has incorporated trade secrets into both its own and a general larceny statute, at least three states (Pennsylvania, Massachusetts and Illinois) have incorporated trade secret protection into theft or larceny statutes without denominating abuse of trade secrets as a separate offense from theft or larceny generally. Ordinarily, trade secret protection can be incorporated into theft or larceny statutes in three ways: (1) consolidation of theft of trade secrets into a theft or larceny statute, as in Pennsylvania; (2) definition of trade secret theft as larceny, as in Massachusetts; or (3) inclusion of trade secrets in lists or property protected by larceny statutes, as in Illinois.

8. Privacy Invasions

Almost every state has one or more statutes proscribing invasions of privacy by persons in the public sector. Bills, pending in some states, may affect the private sector as well. Some of these statutes carry criminal penalties that may be invoked when an unauthorized and willful disclosure of personal information is made from a computer data base.

C. FEDERAL PENAL LAWS

1. Computer-Related Crime Laws

As of this date, no federal computer-related crime law has been enacted. The proposed Federal Computer Systems Protection Act of 1979, S. 240 (Appendix C), introduced by Senator Ribicoff, is discussed below. However, 40 sections of Title 18 of the United States Code, provisions of the Electronic Funds Transfer Act, Title XX of FIRA, and provisions of the Privacy Act of 1974 have direct utility to federal prosecutions of computer abuse.

2. Proposed Computer-Related Crime Laws

Summary -- The Federal Computer Systems Protection Act of 1979, S. 240, was originally introduced by Senator Ribicoff as S. 1766. Hearings were held in June 1978, and the bill was modified and reintroduced as S.240 in the current Congress in its present form. Further revisions may be incorporated to reflect recommendations by the Department of Justice and by The Senate Judiciary Subcommittee.

S. 240 proscribes acts to computers that are in whole or in part operated in interstate commerce or owned by or under contract to or in conjunction with any financial institution, any agency, branch, or department of the U.S. government, or any entity operating in or affecting interstate commerce done for the purpose of either devising or executing a scheme to defraud or obtain property, money, or services by false pretenses or intentionally and without authorization directly or indirectly accessing, altering, damaging, destroying, or attempting to destroy such computers (systems, networks).

The penalty for the fraud aspects of the bill is 2-1/2 times the amount of the fraud, or up to 15 years in prison, or both. The penalty for unauthorized acts is a fine of up to $50,000, or 15 years in prison, or both.

3. Other Authority Bearing on Computer-Related Crime

a. Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA)

Title XX of FIRA is the Electronic Fund Transfer Act ("the Act"). Its primary objective is to define and provide for individual consumer rights as they are affected by EFT. In so doing, the Act provides federal regulation of EFT by establishing the rights, liabilities, and responsibilities of participants, including financial institutions, consumers, and other users of EFTS.

Section 916 of the Act is the criminal liability section, which most directly concerns or at least may have a bearing on computer crime in the federal arena. It provides for a fine of not more than $5,000,

imprisonment for not more than 1 year, or both for anyone who knowingly and willfully gives false information or fails to provide information required by the Act or regulations promulgated thereunder, or otherwise fails to comply with the Act or its regulations.

The second section of the criminal liability provision imposes a fine of not more than $10,000, imprisonment for not more than 10 years, or both for the following 6 acts when interstate or foreign commerce is involved, when the money, goods, services, or things of value involved have a value of $1,000 or more when aggregated over a 1 year period and when a counterfeit, fictitious, altered, forged, lost, stolen, or fraudulently obtained debit instrument is involved. The term "debit instrument" means a card, code, or other device by which a person may initiate an EFT. The 6 acts include:

- o Knowingly using or attempting or conspiring to use a debit instrument, as described above, to obtain anything of value, as described above
- o With unlawful or fraudulent intent, transporting or attempting or conspiring to transport a debit instrument knowing that it is counterfeit, stolen, etc.
- o With unlawful or fraudulent intent, using an instrumentality of interstate or foreign commerce to sell or transport a debit instrument knowing it is counterfeit, stolen, etc.
- o Knowingly receiving, concealing, using, or transporting anything of value (except tickets for interstate or foreign transportation) which has moved in interstate or foreign commerce and has been obtained with a counterfeit, stolen, etc., debit instrument
- o Knowingly receiving, concealing, using, selling, or transporting one or more tickets for interstate or foreign transportation whose value aggregated within a 1 year period is $500 or more and was obtained or purchased by means of a debit instrument that was counterfeit, stolen, etc.
- o In a transaction affecting interstate or foreign commerce, furnishing anything of value through the use of a counterfeit, stolen, etc. debit instrument knowing that it is counterfeit, stolen, etc.

b. The Federal Privacy Act of 1974

The Privacy Act of 1974 is codified in 5 U.S.C. # 552a. The criminal penalties for violation of its provisions are contained in subsection (i)(1)-(3). These criminal penalties may be invoked when a violation of the Act, resulting from an unauthorized and willful disclosure of personal information, is made from a computer data base.

The basic provisions of the Act are to protect the privacy of individuals. Therefore, an agency, as defined in 5 U.S.C. ## 551(1) and 552(e), is prohibited, with a variety of exceptions, from disclosing any record contained in a system of records to anyone or another agency unless the individual has made a written request or has given prior written consent.

If any officer or employee of an agency, knowing that disclosure of specific material is prohibited either by the Act or regulations promulgated thereunder, willfully discloses the material to a person or agency not entitled to it, the officer or employee has committed a misdemeanor and will be fined not more than $5,000.

The same penalty is applicable to an officer or employee who willfully maintains a system of records, which could include a computer data base, without complying with the notice requirements of Subsection (e)(4). Subsection (e)(4) requires each agency that maintains a system of records to publish in the Federal Register not less than once a year a notice of the existence and character of the record system. The notice must include the system's name and location, the categories of individuals, records and their sources included, the routine use of the records, the system's storage, retrieval, access control and disposal policies and practices, the responsible agency official, procedures used to notify individuals, at their request, that records are contained regarding that individual and procedures for an individual to gain access to the records and to contest the contents of the records.

Finally, the same criminal penalties are applicable to anyone who knowingly and willfully requests or obtains under false pretenses a record regarding an individual.

c. Federal Copyright Act

Theft of computer programs can be prosecuted under federal copyright laws. The copyright office has accepted registration of computer programs as "books" since 1964. The House Committee Report on the Copyright Act of 1976, p. 54, states that the term "literary works...includes computer data bases, and computer programs to the extent that they incorporate authorship in the programmer's expression of original ideas, as distinguished from the ideas themselves." Thus authors of computer programs can protect documentation and lines of computer code from copying, but copyright protection does not extend to programmer's algorithms.

In addition to providing for civil actions and damages for copyright infringement the Copyright Act of 1976 also provides for criminal penalties for infringement and for fraudulent removal of copyright notice. Criminal liability for infringement is proven by showing the elements of civil infringement, ownership in another party and copying, and, in addition, by demonstrating willfulness and financial gain. (17 USC #506(2)) Section 506(a) provides for a maximum

penalty of 1-year imprisonment and a $10,000 fine. Section 506(b) also provides for a mandatory forfeiture and destruction of all infringing copies.

Section 506(d) makes it a criminal act to remove or alter any notice of copyright with a fraudulent intent. This conduct is criminal even though it creates no civil liability. Anyone convicted of such an act is subject to a $2,500 fine.

State laws purporting to describe criminal or lawful conduct involving copyright infringement under federal laws are invalid under the doctrine of federal preemption.

4. Federal Criminal Code Provisions

At least 40 sections of Title 18 of the United States Code bear directly or indirectly on computer abuse. For ease of analysis, these are grouped into seven broad categories: theft and related offenses; abuse of federal channels of communication; national security offenses; trespass and burglary; deceptive practices; property damage; and miscellaneous.

a. Theft and Related Offenses

18 U.S.C. # 641 (Embezzlement or Theft of Public Money, Property, or Records) -- The basic statute that protects federal property from theft is 18 U.S.C. # 641. The statute covers both the thief and the receiver of stolen property. Although most of the terms of the statute are straightforward, several bear directly on computer abuse because of their expansive meanings.

(a) One who "knowingly converts" public property violates # 641. It is no defense to a charge of unlawful conversion that one intended to return the property, cf. Morissette v. United States, 342 U.S. 246 (1952). "[C]onversion...may be consummated without any intent to keep..." 342 at 271-272, or make restitution, unless those acts negate the requisite mens rea. While no court has ever considered whether one may "embezzle," "steal," or "purloin" programs by unprivileged copying or otherwise, it is highly likely that any unprivileged abuse may be styled a "conversion."

> Conversion, however, may be consummated without any intent to keep and without any wrongful taking, where the initial possession by the converter was entirely lawful. Conversion may include misuse or abuse of property. It may reach use in an unauthorized manner...It is not difficult to think of intentional and knowing abuses and unauthorized uses of government property that might be knowing conversions but which could not be reached as embezzlement, stealing or purloining. Knowing conversion adds significantly to the range of protection of government property...342 U.S. at 271-

272. See also United States v. Tijerina, 407 F.2d 349 (1-th Cir. 1969), cert. den. 396 U.S. 843 (1969), (deprivation of control of trucks for a period of time an unlawful conversion within # 641).

(b) The notion of "conversion" is as broad as the definition of the res which is public property. Moreover, the statute itself is broad enough to include theft of labor or services, Burnett v. United States, 222 F.2d 426 (6th Cir. 1955), (wrongful conversion of services and labor to two army servicemen by army officer), and uses the catch-all phrases "any...thing of value..."

(c) The meaning of the phrase "of the United States or of any department or agency thereof" is broader than absolute ownership. An agency of the United States is, among other things, "any corporation in which the United States has a proprietary interest...;" 18 U.S.C. # 6. "Proprietary interest" is broad enough to include any ownership of stock. Cf. United States v. Anderson, 45 F. Supp. 943, 946 (S.D. Cal. 1941) (discussing predecessor to # 641). It may be enough if the United States has the power to control the use of the res, Bernhardt v. United States, 169 F.2d 983 (6th Cir. 1948) (property under Army control at Army depot protected by # 641), even if the res is in private hands. United States v. Echevarria, 262 F. Supp. 373 (D.P.R. 1967) (advances of United States funds paid to university are protected by # 641). Although there are no cases directly on point, it seems clear that a joint interest, divided or undivided, or an equitable interest, such as a right to use, may be converted. Thus, should the government purchase the right to use certain programs, and those programs be misappropriated, prosecution should be available under # 641. In addition, there is one case that suggested that property in government custody or possession, even if the government has no legal or equitable title thereto, may be the subject of theft. See United States v. Gardner, 42 F. 829 (N.D. N.Y. 1890) (custom booty awaiting foreclosure as res subject to theft).

(d) It is clear that if programs are being developed for the government, their theft or conversion violates # 641. Moreover, United States v. Anderson, shows that raw materials may well be included under this clause. 45 F. Supp. at 945-949.

In its broadest interpretation, any misappropriation of programs that are subject to some measure of government control, custody, or ownership is a violation of # 641.

Two recent decisions have dealt with 18 U.S.C. # 641. United States v. Digilio, 538 F.2d 972 (3d Cir. 1976), was a conviction for conspiracy to defraud the United States and to convert to the defendant's own use the records of the United States, particularly photocopies of official files of the FBI. Defendants contended that # 641 was inapplicable because the government was not deprived of the use of the information contained in the records. They contended that the

unauthorized copies of government records were not themselves records and that the unauthorized transmission of the information is not proscribed by # 641.

The government had based its argument of # 641 applicability on United States v. Bottone, 365 F.2d 389 (2d Cir. 1966) cert. den. 385 U.S. 974, 87 S. Ct. 514, 17 L. Ed. 2d 437 (1966), which held that microfilming of scientific processes with the thief's own equipment and asportation of those copies were proscribed as theft of "goods." The court in agreeing with the government's position, noted that, in Digilio, there was no memorization of the information nor copying by the use of the thief's own equipment. One of the criminals actually used government time, equipment, and supplies to make the copies. Finally, the court stressed that a duplicate copy is a record for purposes of the statute and duplicate copies belonging to the government were stolen.

In United States v. Lambert, 446 F. Supp. 890 (D. Conn. 1978), a # 641 (larceny) case, the defendants were charged with selling information derived from a computer within the Drug Enforcement Administration, Washington, D.C. The information included the identity of informants and the status of government investigations into illegal drug traffic. Only the information, not the documents containing the information, were transferred. The defendants contended that # 641 was applicable only to tangible items, e.g., documents embodying the information, not the information itself. However, the court held that the open-ended "thing of value" phrase of the statute evidences an intent to cover a wide variety of conduct.

The court saw no reason to restrict the interpretation of # 641 to its common law origins. It held that # 641 should cover larceny as well as any new situations that may arise under changing modern conditions and not envisioned under the common law. The court agreed with the government that the property involved was highly sensitive and confidential information maintained in computer records and had a value only so long as it remained in the government's exclusive possession. It thus held that the phrase "thing of value" in conjunction with the explicit reference to records in # 641 covers the content of such record.

18 U.S.C. # 659 (Theft of Goods or Chattels Moving as, Which Are Part of, or Which Constitute Interstate Commerce) -- Programs may be sent by interstate common carrier. When they are, # 659 protects them from theft, irrespective of ownership. Unlike # 641, # 659 does not seem to proscribe unauthoized copying per se of programs. Although the statute uses "conversion," it is relevant only to the intent of the actor, and not his act, which must be embezzlement, stealing, etc. The most interesting question posed by # 659 concerns theft from interstate commerce.

An excellent discussion of the elements and breadth of what constitute interstate commerce in # 659 is found in United States v. Astolas. 487 F.2d 275 (2d Cir. 1973). In rejecting appellant-defendants' claim that the trucks they hijacked were not yet, or had ceased to be, part of interstate commerce, Judge Medina quoted with approval the trial court's instruction:

> The interstate character of a shipment commences at the time the property is segregated for interstate commerce and comes into possession of those who are assisting its course in interstate transportation and continues until the property arrives at its destination and is there delivered either by actual unloading or by being placed to be unloaded. 487 F.2d at 278.

The requirement of the existence of interstate commerce relates to the time of the theft, United States v. Tyers, 487 F.2d 828, 830 (2d Cir. 1973), so that one who steals a program may not pass it off later to an accomplice leaving the accomplice immune. Nor is it essential that the program ownership be by common carrier to be protected; it is clear that # 659 covers carriage by the owner. Winer v. United States, 228 F.2d 944, 947 (6th Cir. 1956), cert. den. 351 U.S. 906 (1956). It is equally clear that interstate commerce does end sometime, cf. O'Kelley v. United States, 116 F.2d 966 (8th Cir. 1941) (theft from boxcar after delivery and partial unloading), but so long as initial steps have been undertaken, cf. United States v. Sherman, 171 F.2d 619 (2d Cir. 1948) (labeling and delivery of bales of duck canvas to wharf), the program is en route, cf. United States v. Maddox, 394 F.2d 297 (4th Cir. 1968) (brief pauses in interstate journey are included within # 659), or yet to be unloaded, # 659 is applicable.

18 U.S.C. # 2314 (Interstate Transportation of Stolen Property) -- Unlike # 659, # 2314 apparently requires that the stolen property cross state lines. It does not seem sufficient merely for the stolen property to be introduced into interstate commerce. Although there are no reported cases directly on point, that is, where the stolen proprty was delivered to an interstate carrier but did not actually cross state lines, statutory analysis in United States v. Roselli 432 F.2d 879, 891 (9th Cir. 1970), supports this conclusion. In Roselli, the court contrasted the antiracketeering statute, 18 U.S.C. # 1952, with # 2314, noting that use of interstate facilities or participating interstate travel was sufficient to provide jurisdiction for the former, while failing to assert that use of interstate facilities was sufficient to trigger the latter. Moreover, reported cases, involving # 2314, have all involved the crossing of state lines. See, e.g., United States v. Sheridan, 329 U.S. 379 (1946) (causing fraudulent check to cross state lines); United States v. Hassel, 341 F.2d 427 (4th Cir. 1965) (causing victim of confidence game to cross state line); United States v. Jacobs, 485 F.2d 270 (2d Cir. 1973) (causing stolen Treasury bills to cross state lines).

The major issue raised by # 2314 is whether a copy of a program stolen, converted, or taken by fraud and transported across state lines can trigger # 2314. The only reported case of a copy used in a related prosecution is United States v. Lester, 282 F.2d 750 (3d Cir. 1960), cert. den. 364 U.S. 937 (1961). In Lester, a co-conspirator made numerous copies of valuable geophysical maps, transported the copies across state lines, and appellant was arrested and convicted for conspiring to transport stolen maps in interstate commerce. Rejecting appellant's claim that copies were not stolen property, the court held that the property stolen was the valuable idea, not the paper embodiment. 282 F.2d at 755.

Although the court in Lester found no need to elaborate upon its holding, it could have cited United States v. Handler, 142 F.2d 351 (2d Cir. 1944), cert. den. 323 U.S. 741 (1944), the most thorough analysis to date of stolen property. After analyzing other case law, the meaning of "stealing," and the legislative history of the National Stolen Property Act, now # 2314, the court in Handler concluded:

> (1) the stolen proprty need not be taken larcenously, that is, there are no requirements of asportation, tangibility, etc.; and (2) 'the statute is applicable to any taken whereby a person dishonestly obtains goods or securities belonging to another with the intent to deprive the owner of the rights and benefits of ownership.'" 142 F2.d at 353. Since a copy of a program will indeed deprive the rightful owner of the benefits of ownership, a copying should create the stolen property necessary to trigger # 2314.

Note, however, that in United States v. Seidlitz, No. 76-2027 (4th Cir. 1978), the trial judge dismissed a count based on # 2314 because what crossed state lines was electronic signals, which he concluded were not property. Seidlitz was convicted of wire fraud.

In re Vericker, 446 F.2d 244 (2d Cir. 1971), was a contempt conviction against a defendant who would not testify before the grand jury even after having been granted transactional immunity. The problem was that the defendant was granted transactional immunity as to ## 2314 and 2315 only. The immunity, however, was not applicable to the crimes suggested by questioning of the prosecutor. Sections 2314 and 2315 deal with the theft and receipt of stolen goods, wares, merchandise, securities or money, not FBI documents, which the prosecutor had been interested in. Although the court admitted that in some circumstances mere papers may constitute goods, wares, and merchandise, citing United States v. Bottone, 365 F.2d 389 (2d Cir. 1966) cert. den. 385 U.S. 974, 87 S. Ct. 514, 17 L. Ed. 2d 437 (1966), such papers must be well within the normal meaning of goods, wares, or merchandise, that is, property that is ordinarily the subject of commerce. Thus, geophysical maps or secret manufacturing processes are ordinarily the subject of sale and/or license. However, papers showing that individuals are or may have been engaged in criminal activity or what procedures are used by the FBI in

tracting them down are ordinarily not bought or sold in commerce, and, therefore, the government did not show that its questions regarding the theft of FBI documents were related to # 2314 and 2315, and, therefore, could supersede the defendant's invocation of the 5th Amendment privilege.

In United States v. Greenwald, 479 F.2d 320 (6th Cir. 1973) cert. den. 414 U.S. 854, 94 S. Ct. 154, 38 L. Ed. 2d 104, the Court addressed the issue whether secret chemical formulae or formulations fall within the statutory language of # 2314 "goods, wares, or merchandise." In Greenwald, the number of documents containing the formulations was restricted for purposes of competitive advantage, but one set was given to the defendant, a chemical engineer in the sales department, who appropriated them. The testimony at the trial showed that there was an established market for the chemical formulae and formulation, that is, manufacturers shared formulae by sale or license and treated such as assets similar to machinery or equipment. The court cited United States v. Bottone, 365 F.2d 389 (2d Cir. 1966) cert. den. 385 U.S. 974, 87 S. Ct. 514, 17 L. Ed. 2d 437 (1966) and In re Vericker, 446 F.2d 244 (2d. Cir. 1971), to hold that, given an established, viable, although limited market in chemical formulation, the lawful appropriation of original documents containing such formulations fell within the meaning of # 2314 because the formulations were "goods, wares or merchandise."

United States v. Drebin, 557 F.2d 1316 (9th Cir. 1977), was a case in which the defendants contended that motion picture photo plays were intangible and could not be considered "goods, wares, or merchandise" under 18 U.S.C. # 2314. The defendants' arguments consisted of claiming that copyrights were intangible property rights, separate and distinct from property rights in the tangible item from which copies are made, and that a copy cannot be acquired by theft, conversion, or fraud because the copyright owner has no proprietary interest in the duplicate of his work. The court rejected these contentions as illogical and contrary to law and held that the copies are goods or merchandise for the purpose of # 2314. Moreover, the court held that the illicit copying of a copyrighted work is no less an offense than if the original were taken.

Finally, in United States v. Jones, 414 F. Supp. 964 (D. Maryland 1976), the defendant was charged with transportation in interstate commerce of stolen, converted, or fraudulently obtained securities under 18 U.S.C. # 2314. The defendant claimed that the securities were forgeries and not "securities," noting that # 2314 was not applicable to falsely made, forged, altered, or counterfeited representations of obligations of foreign governments or banks or corporations of foreign governments.

The checks complete with signatures, were printed by computer as the result of tampering by the employee with the data records stored in the computer. The procedure that the employee used was first to enter an improper vendor code listing, then to enter data regarding the

specific checks to be issued to that false vendor, then to forward to key punch the documents and accounts payable slips, and finally to command from the computer the processing of a check run where the computer would automatically print the checks to the false vendor. The issue before the court was whether these checks consitututed forgeries and thus the denfendant's conduct inapplicable for punishment under 18 U.S.C. # 2314. The court noted that where falsity in the instrument is in the content rather than the manner of making the instrument, it is not a forgery. In this case the checks were not lies "in writing," but rather the unauthorized issuance thereof. The court held that the mere fact that a computer was used was not relevant because it was simply an inanimate and obedient instrumentality used by the employee similar to a check-writing machine or ballpoint pen and thus was not a forgery.

18 U.S.C. # 661 (Theft Within Special Maritime and Territorial Jurisdiction) -- When programs are stolen in a federal enclave as defined in 18 U.S.C. # 7, a violation of # 661 occurs. As in ## 641 and 2314, the question again arises whether unauthorized copying is a violation of the statute. Although it was assumed, for analytical purposes, earlier that copying is not within the scope of # 661, a broad reading of the statute may well include it. In United States v. Henry, 447 F.2d 283 (3d Cir. 1971), appellant was convicted for stealing a boat within the maritime jurisdiction. On appeal, it was argued that the statute was merely a codification of common law larceny, and since the government failed to offer proof that appellant intended to permanently deprive the owner of his property, the conviction should be overturned. In rejecting appellant's claim, the court held that the statute was broader than common law larceny. Drawing on the 2nd Circuit's definition of "to steal" in Handler, the court concluded that when one "willfully obtains or retains possession of property belonging to another without the permission or beyond any permission given with the intent to deprive the owner of the benefit of ownership," 447 F.2d at 286, an offense was made out under # 661. As noted earlier, the "deprivation of benefit" theory should enable a prosecutor to support an indictment for unauthorized copying.

b. Miscellaneous Theft and Theft-Related Offenses

(a) Although there is no general federal statute prohibiting theft by false pretenses, except 18 U.S.C. # 1025 (false pretenses within the special maritime and territorial jurisdiction) and # 287 (making false claim to United States), courts have construed # 641 to include false pretenses. See Burnett v. United States; Morgan v. United States, 380 F.2d 686 (9th Cir. 1967) (tax fraud as theft of government money by false pretenses). Thus, there seems no bar to charging one who fraudulently obtains computer usage from the United States, while stealing programs, with a violation of # 641.

(b) Many theft statutes, such as # 641, 659, and 2314, have receiving stolen property provisions as well. In addition, # 662 prohibits receiving stolen property within the special maritime and

territorial jurisdiction. Section 2315 proscribes the receipt of goods stolen from interstate commerce. Thus, one who induces the theft of programs not only may be charged as a principal, 18 U.S.C. # 2, or as a conspirator, 18 U.S.C. # 371, but also may run afoul of the foregoing sections.

(c) Numerous federal statutes designed to cover specific types of theft, but they may be applicable to certain instances of program abuse. For instance, if one has the misfortune to steal a program used in the payment of government money, he violates # 285 that deals with taking or using papers relating to claims. If a government employee wrongfully converts, cf. Morissette v. United States, the property of another which is entrusted to him, he commits an offense under 18 U.S. C. # 654. This section would be particularly effective when the employee provided a copy to an unauthorized third party. Theft of programs from federally insured banks and financial institutions is covered by 18 U.S.C. ## 655-657, although there is some doubt as to whether nonmonetary property is covered by # 656 because the protected res is "moneys, funds or credits," in contrast to "other property of value." 18 U.S.C. # 657. But this loophole is closed by 18 U.S.C. # 2113(b) which covers the theft of "any property...any other thing of value..." from a bank or savings institution. And finally, if a thief "steals, purloins, or embezzles" property "used" by the Postal Service, he violates # 1707.

c. Abuse of Federal Channels of Communication

18 U.S.C. # 1341 (Mail Fraud) -- The mail fraud statute has two essential elements: (1) one must use the mail for the purpose of executing or attempting to execute, (2) a fraud or a scheme to obtain money or property under false pretenses. The courts have been generous in their definition of what is a fraud. The classic statement on this count was made by Judge Holmes, "[t]he law does not define fraud; it needs no definition; it is as old as falsehood and as versatile as human ingenuity." Weiss v. United States, 122 F.2d 675, 681 (5th Cir. 1941), cert. den. 314 U.S. 687 (1941) (construction scope of fraud in predecessor to # 1341. Weiss was quoted with approval in Blachly v. United States, 380 F.2d 665 (5th Cir. 1967) (referral selling plan as fraud) and United States v. States 362 F. Supp. 1293 (E.D. Mo. 1973) (ballot box fraud in primary election as mail fraud), aff'd 488 F.2d 761 (8th Cir. 1973) (see cases cited therein), cert. den. 417 U.S. 909, 417 U.S. 950 (1974).

Thus, the thrust of the various court opinions would include any scheme to copy programs as a scheme to defraud, and any mailing in furtherance of the scheme would trigger the statute. If the thief uses a mailing to defraud a computer center through services, labor, credit, etc., United States vs. Owens, 492 F.2d 1100 (5th Cir. 1974) (mailings which led to receipt of goods on credit as mail fraud), or uses the mailing to obtain the program itself, he falls within the scope of # 1341. The prosecutor should always explore # 1341's applicability in any instance of computer abuse. For a prosecutor's opinion of the

effectiveness of $ 1341 and, in contrast, the ineffectiveness of the Proposed Code. [See Givens, The Proposed New Federal Criminal Code, 43 N.Y. St. B.J. 486, 488-494 (1971) et passim.

18 U.S.C. # 1343 (Wire Fraud)--The elements of # 1343 are identical to $ 1341, with the exception of the federal medium abused. When one uses a remote terminal to perpetuate a computer fraud, or when one telephones an accomplice, so long as the "message" crosses state lines, the statute is applicable. All reported cases involving # 1343 have dealt with conversations that crossed state lines, leading one to believe that the message must, in fact, cross state lines. Since # 1343 does not use the word "facility," jurisdiction hinges on use of an interstate wire, notwithstanding the fact that "[I]t cannot be questioned that the nation's vast network of telephone lines constitute interstate commerce." United States v. Holder, 302 F. Supp. 296, 298 (D. Mont. 1969). It is not clear that the use of the word "facility" in any new legislation would embrace interstate calls either, see United States v. DeSapio, 299 F.Supp. 436, 448 (S.D.N.Y. 1969) (construing phrase "facility in . . . interstate commerce" as requiring interstate calls for 18 U.S.C. # 1952), because there may be a distinct difference between facilities "in" interstate commerce and facilities "of" interstate commerce. Both mail fraud and wire fraud are very useful aids to the prosecution of computer crime.

d. National Security Offenses

18 U.S.C. # 793 (Gathering, Transmitting, or Losing Defense Information)--This section, and those which follow in this category, is of limited use in software abuse. But, as a general rule, whenever abuse involves classified, restricted, or defense programs, these sections should be inspected for applicability. Section 793 is broad in scope; Subsection (a), the geographical intrusion provision, covers property owned, controlled, or used by contractors of the government when the property is related to or connected with national defense. The section also proscribes copying of defense information, unlawful reception, communication of contents, and grossly negligent losses. This statute has been held sufficiently definite to satisfy due process requirements, Gorin v. United States, 312 U.S. 19(1941), and has been held to encompass "related activities of national defense" as well as military enclaves. 312 U.S. at 28. See also United States v. Drummond, 354 F.2d 132, 151 (2d Cir. 1956) (upholding jury charge in same language).

18 U.S.C. # 794 (Gathering or Delivering Defense Information To Aid Foreign Government)--This statute provides more severe penalties for actual transmission of the defense information to a foreign government and also includes a conspiracy count. One caveat should be mentioned in this discussion of ## 793 or 794, or companion statute # 798, which deals with disclosure of classified information. Although it has always been true that public information is outside the scope of the protected

res, see Gorin v. United States; see also United States v. Heine, 151 F.2d 813 (2d Cir. 1945) (officially disseminated information, no matter how painstakingly culled and digested, is not "defense information"), the Pentagon Papers case, New York Times Co. v. United States, 403 U.S. 713 (1971), now makes it clear that mere classification is not enough. The flavor of the Black, Douglas, Brennan, and Marshall opinions is that, even in criminal prosecutions, lack of substantial injury to national security might be a valid defense. Eventhough it is true that White and Stewart contrasted civil injunctive (unpermitted) and criminal (permitted) sanctions, there is language, in the Stewart opinion that hints at a need for narrowly construed guidelines on classification. Thus, a clear majority in the case would seem to support the proposition that classified material that had no business being classified, such as information related to Department of Defense lobbying efforts, could not support a prosecution under Chapter 37 of Title 18.

18 U.S.C. # 795 (Photographing and Sketching Defense Installations)--In 1950, President Truman declared pursuant to # 795, that all military and commercial defense establishments were to be protected against unauthorized photographing and sketching. Exec. Order 10104, 15 Fed. Reg. 597, 598 (February 1, 1950). Since the statute covers "graphical representations" of classified "equipment," it is probable that copying classified programs would fall within this section.

18 U.S.C. ## 797, 798, 799, and 952--Section 797 deals with subsequent publication and sale of photographs or sketches of equipment denominated in # 795. Section 798, which deals with codes and cryptographic systems, would be pertinent in any abuse from agencies involved in communications work. Section 799 deals with security violations of NASA regulations, and # 952 deals with disclosure of diplomatic codes.

e. Trespass and Burglary

Criminal Trespass -- There is no general federal statute covering criminal trespass. In fact, the only statute that denominates trespass a crime in Title 18 is # 2152, dealing with trespass on fortifications or harbor-defense areas. Section 2278(a) of Title 42 forbids trespass on installations of the Atomic Energy Commission (ERDA). Neither is particularly applicable to trespass for the purpose of misappropriating programs, unless the situs of the trespass is a fortification, harbor-defense area, or DoD installation.

Burglary -- The federal burglary statutes are slightly more comprehensive, but not much. Title 18 provides criminal penalties for burglary of a bank, 18 U.S.C. # 2113(a), post offices, 18 U.S.C. # 2115, and interstate carrier facilities. 18 U.S.C. # 2117.

(a) 18 U.S.C. # 2113(a) (Burglary of a Bank). Although some states have denominated copying of trade secrets as larceny, it seems doubtful that entry of a bank to copy programs would make out a federal crime, notwithstanding the language "or any larceny" of # 2113(a). United States Rogers, 289 F.2d 433, 437 (4th Cir. 1961) (the language of the statute refers only to common law larceny), The U.S. Supreme Court has rejected a claim that federal criminal law in this case turns on state law. Jerome v. United States, 318 U.S. 101, 106 (1943) (state felonies irrelevant). Once beyond those restrictions, however, the statute is effective against the most traditional defenses. Privileged entry is no defense, see Audett v. United States, 132 F.2d 528, 529 (8th Cir. 1942) (entry may include "walking in [with] a stream of customers through the front door...in business hours"), nor is breaking an element of the offense. Although burglary statutes were originally designed to protect occupied spaces from crime, occupancy is irrelevant for purposes of # 2113(a). United States v. Poindexter, 293 F.2d 329 (6th Cir. 1961) cert. den. 368 U.S. 961 (1962).

(b) Unlike # 2113(a), 18 U.S.C. # 2115 (burglary of post offices) requires forcible breaking as an element of the offense. The only vague term in the statute is "depredation." While the parameters of the term are hazy, depredation is generally held to mean plundering, robbing, or pillaging. See Deal v. United States, 274 U.S. 277, 283 (1927) (construing similar language in postal regulations).

Similar to # 2115, 18 U.S.C. # 2117 (burglary of interstate carrier facilities) also requires a breaking. Again, mens rea is intent to commit larceny, which would be common law larceny.

f. Deceptive Practices

18 U.S.C. # 912 (Obtaining Thing of Value by Impersonating an Officer or Employee of the United States)--It may often be the case that one who misappropriates software within a federally protected sphere has falsely represented himself as a government officer or employee in order to gain access to the program. There is no requirement that the "thing of value" be tangible, cf. United States v. Lepowitch, 318 U.S. 702 (1943) (fraudulent acquisition of information about whereabouts of another), and a copy of the program would certainly seem to fall within the definition. The statute must be read broadly to encompass new concepts of "thing of value" for " it was not possible for Congress in enacting the statute to anticipate all devices and schemes which human knavery might conceive in security benefits..." United States v. Ballard, 118 F. 757 (D.Mo. 1902) (meals and lodging are a thing of value).

18 U.S.C. # 1001 -- When # 1001, the catch-all that deals with all manner of false representations, is compared with # 912, it becomes apparent that the general rule statute carries a much more severe

penalty than the specific statute. In addition, # 1001 requires no fraudulent obtaining of a thing of value; a false, fictitious or fraudulent statement, knowingly and willfully made, is enough to trigger the statute. Whatever one may say about the jurisprudential wisdom of the statute, it seems applicable to almost every instance of computer abuse in the federal sphere. For example, programs may not be divulged to unauthorized persons. 5 U.S.C. # 552(b)(4) (trade secrets subsection of Freedom of Information Act). Therefore, one who fails to identify himself as unauthorized conceals a material fact, whether or not he represents himself as unauthorized. Is active misrepresentation a less serious crime? Moreover, this section applies to both oral and written misrepresentations. See United States v. Zavala, 139 F.2d; 830 (2d Cir. 1944) (false oral and written customs declaration). It may even be applicable to electronic signals from a remote terminal that falsely represent the sender as one authorized to protected software.

18 U.S.C. ## 1005,1006 (False Entries in Records of Banks and Credit Institutions)--Whenever anyone makes a false entry in a bank or credit institution record, with intent to injure or defraud, he runs afoul of ## 1005 or 1006. Although both of the statutes are quite fact-specific, they are comprehensive in their respective areas. Since the purpose of the statutes was to ensure correctness of bank records, United States v. Giles, 300 U.S. 41, 48 (1937) (teller's failure to file deposit slips is equivalent to the making of a false entry), active or passive omissions or commissions are covered.

Considering the purpose noted above, that is, to ensure correctness of bank records, the breadth with which "bank books" has been interpreted, cf. Lewis v. United States, 22 F.2d 760 (8th Cir. 1927) (minutes of meetings of board of directors were "bank books"), and the need to protect banks from loss, Weir v. United States, 92 D.2d 634 (7th Cir. 1937), it seems reasonable that computer records should be within the scope of ## 1005 and 1006. Thus, any false entry, obliteration, or alteration of computerized bank records would be a violation of either ## 1005 or 1006.

g. Property Damage

18 U.S.C. # 81 (Arson Within Special Maritime and Territorial Jurisdiction)--Although arson may be only infrequently used as a tactic in computer abuse, the prosecutor should be aware of the scope of the statute. A key question is whether hardware or programs may be included within the phrase "machinery or building materials or supplies." A recent case arising from the Wounded Knee occupation indicates that the definition of the phrase may be narrowly construed. In United States v. Banks, 368 F. Supp. 1245 (D.S.D. 1973), the defendant-appellant was accused and convicted of violating # 81 by burning motor vehicles within a federal enclave. Holding that motor vehicles were not "machinery" within # 81, the court through Judge Nichols, invoked ejusdem generis and noted the broad interpretation of "machinery" would endanger the

statute as too vague, lacking the "requirement of definiteness...that a person of ordinary intelligence must be given fair notice that his contemplated conduct is forbidden..." 368 F. Supp. at 248. Thus, a prosecutor might be advised to style any indictment alleging the burning of hardware of software as, alternatively, an attempt to set fire to a building or structure.

18 U.S.C. # 1361 (Malicious Injury to Government Property)--Several cases construing # 1361 demonstrate the liberality with which various courts have accepted indictments charging injury in cases of malicious mischief. Section 1361 was somewhat of a dead letter until interference with the Selective Service began to mushroom in the 1960's. It was resurrected as a "catch-all" to encompass otherwise unindictable offenses. For instance, in United States v. Eberhardt, 417 F2.d 1009 (4th Cir. 1969), the 4th Circuit considered the famous Baltimore blood-pouring case. Father Philip Berrigan and two others were convicted of violating # 1361 in that they poured blood on Selective Service records. In affirming the convictions, the court utilized the cost of restoring the records as the measure of damages. The appellants did not argue that blood pouring was not "injury" within the meaning of the statute. As a result, the breadth of the case is not clear. At its narrowest, it would mean that any temporary physical obliteration, subsequently restored, is an "injury." While the res in most Selective Service cases was government records at least arguably critical to national defense, other cases construing # 1361 show that neither the injury, nor the res injured need be terribly major. See, e.g., Tillman v. United States, 406 F.2d 930 (5th Cir. 1969) (glass door at induction station broken by draft resistors); Edwards v. United States, 360 F.2d 732 (8th Cir. 1966) (plumbing fixture from vacant home); Brunette v. United States, 378 F.2d 18 (9th Cir. 1967) (dented fender). Putting all of the cases dealing with # 1361 together with the broadest interpretation of Eberhardt may enable a prosecutor to argue successfully that an interference with the use of government software is "injury," and the measure of damage is either the cost of restoration or the cost of development when not restorable.

18 U.S.C. # 1363 (Malicious Injury Within the Special Maritime and Territorial Jurisdiction)--This section differs from # 81 only in its substitution of malicious mischief for arson.

18 U.S.C. # 2071 (Concealment, Removal, or Mutilation of Public Records)--Another statute that was resurrected during the Vietnam-protest era, # 2071 should be effective against misappropriation of computerized government records, especially when a traditional larceny charge cannot be sustained. For example, copying via a remote terminal without subsequent asportation. The bulk of # 2071 cases deal with Selective Service records and documents, see e.g., United States v. Chase, 309 F. Supp. 420 (n.D.Ill. 1970); Chase v. United States, 468 F.2d 141 (7th Cir. 1972); United States v. Donner, 497 F.2d 184 (6th

Cir. 1974); United States v. Eberhardt, and thus it would be extending case law to include computerized records as a "document or other thing." Such an extension is rational. The purpose of # 2071 "is to prevent any conduct which deprives the Government of the use of its documents, be it by concealing, destruction, or removal." United States v. Rosner, 352 F. Supp. 915, 919 (S.D.N.Y. 1972). The res protected by # 2071 is not merely documentary or written records, but any type of public record. Cf. United States v. DeGroat, 30 F. 764 (E.D. Mich. 1887) (emphasizing the thrust of the statute as toward records, not papers). And under the rationale of United States v. Rosner, dumping or obliterating a computerized record surely deprives the government of its use as much as a blood-pouring, United States v. Eberhardt, a burning, United States v. Chase, or a mutilation. United States v. Donner.

Destruction of Property Affecting National Security -- (a) The extreme breadth of what constitutes the protected res in 18 U.S.C. # 2153 (willful injury to war or national defense material during war or national emergency) can be seen in its definition in # 2151. War material includes "all articles, parts or ingredients intended for, adopted to, or suitable for...the conduct of war or defense activities." Since the mind has trouble visualizing what in the computer industry would not fall within the definition, it seems clear, so long as scienter is proved, hardware and software within the "defense" orbit are protected. Although the statute applies during war or national emergency, the national emergency declared by President Truman in 1950, Proc. 2912, 15 Fed. Reg. 9029 (December 16, 1950), apparently still exists. United States v. Achtenberg, 459 F.2d 91 (8th Cir. 1972), cert. den. 409 U.S. 932 (1972).

(b) The only substantial difference from # 2163 is the applicability of 18 U.S.C. # 2155 (willful injury to national defense material), irrespective of war or national emergency.

Further Possibilities -- Although # 1361 may be construed to reach certain interferences with use, at present there is no provision generally applicable to interference with use or "tampering."

h. Miscellaneous Provisions

Derivative Crimes and Conspiracy -- This section covers federal law applications to derivative crimes and conspiracy.

(a) Acts which become criminal only because of the criminal acts of another, derivative crimes, are covered in 18 U.S.C. # 2 dealing with aiding and abetting and # 3 dealing with accesssorial liability. As a general rule, any action prior to the crime that induces the criminal act exposes the one who induced to punishment as a principal. Any action subsequent to the crime in the nature of assistance exposes the assistant to a charge of accessory after the fact. Thus, a third party who induces a theft of software, while not indictable by # 641, is indictable under # 2.

(b) 18 U.S.C. # 371 (conspiracy). While there is no general statute which makes it a crime to defraud the government, it is a crime for two or more persons to conspire to commit any offense or defraud the United States. This leads to an anomaly--the planning of an act, not criminal in itself, may be a crime. The implications for software abuse are enormous. The broad scope of what it means to "defraud" the United States can be seen in the leading case in this area, Haas v. Henkel, 216 U.S. 462 (1910). In Haas, three persons, one of whom was a statistician with the Department of Agriculture, conspired to falsify official reports concerning cotton crops and to divulge confidential information concerning those crops to unauthorized person in order that they might speculate in the cotton market. While there was no allegation of pecuniary loss to the government, the Court rejectd a motion to quash the indictment in a habeas corpus proceeding, holding:

> [I]t is not essential that such a conspiracy shall contemplate a financial loss or that one shall result. That statute is broad enough in its terms to include any conspiracy for the purpose of impairing, obstructing or defeating the lawful function of any department of Government...[I]t must follow that any conspiracy which is calculated to obstruct or impair its efficiency and destroy the value of its operations...would be to defraud the United States by depriving it of its lawful right and duty of promulgating or diffusing the information..." 216 U.S. at 479-480. Accord, United States v. Johnson, 383 U.S. 169, 172 (1966) (conspiracy by two congressmen to influence the Justice Department).

A minor and somewhat redundant conspiracy statute, in the light of the gloss Haas puts on # 371, is 18 U.S.C. # 286 dealing with a conspiracy to defraud by payment or allowance of false claims.

18 U.S.C. # 1905 (Disclosure of Confidential Information)--This section is potentially applicable to computer abuse in two types of situations: (a) Where a government officer or employee discloses or communicates the contents of programs in government custody but owned by a private person; and (b) Same as (a), but where the government owns the programs.

(a) Obviously, the Trade secrets of # 1905, makes the disclosure of "custodial" programs an act illegal unless the disclosure is "authorized by law." For purposes of # 1975, a trade secret is "...an unpatented, secret, commercially valuable plan, appliance, formula or process, which is used for the making, preparing, compounding, treating, or processing of articles or materials which are trade commodities." United States ex. rel. Norwegian Nitrogen Products Co. v. United States Tariff Commission, 51 App. D.C. 366, 6 F.2d 491, 495 (1922), rev'd on other grounds, 274 U.S. 106 (1927). See also Consumers Union of U.S. Inc. v. Veterans Administration, 301 F. Supp. 796 (S.D.N.Y. 1969) (raw data compiled by government agency not a trade secret of companies providing data). The only law presently requiring wholesale disclosure of

information is the Freedom of Information Act, 5 U.S.C. # 552, 871 Stat. 56 (1967); however, it does not apply to disclosure of matters which are trade secrets. 5 U.S.C. # 552(b)(4).

(b) Disclosure of government computer programs. It appears that if the government develops its own programs, such programs must be divulged on demand unless they are classified, 5 U.S.C. # 552(b)(1), or a trade secret. In reality, agencies have been loath to divulge their staff-prepared programs. See, Comment, Public Access to Government-Held Computer Information 68 N.W. U.L. Rev. 433, 452 (1973). Whether this reluctance is enough to make them trade secrets is doubtful. See Shapiro v. S.E.C., 399 F. Supp. 467 (D.D.C. 1972) (staff-prepared report on off-board stock trading not "trade secret" within 15 U.S.C. # 552 and not prevented from disclosure by 18 U.S.C. # 1905). Indeed, under the definition in United States ex rel. Norwegian Nitrogen Products v. United States Tariff Commission, it seems hard to imagine the government having its own "trade secret," unless it is engaged in a marketing operation. Thus, it seems that any disclosure made pursuant to a 15 U.S.C. # 552 request would exempt the actor from # 1905 liability.

18 U.S.C. # 701 (Unauthorized use of identification)--This section, closely akin to those grouped under deceptive practices, will reach the offender who utilizes any type of false identification in his misappropriation or attempt to misappropriate.

SECTION VI OVERVIEW OF COMPUTER TECHNOLOGY

This section presents an overview of the technical aspects of computers starting with number representations and what makes a computer work. It includes computer program concepts, computer systems structure, the modes of operation, and data communication. The purpose is to provide investigators and prosecutors unfamiliar with computer technology with basic concepts and a brief review for those more familiar with the technology. This section of the manual and the glossary at the beginning of the manual also can be used as a convenient reference for technical terms and concepts discussed elsewhere.

Prosecutors and investigators will probably seldom encounter cases requiring the detailed information presented here. If they do have such cases, expert assistance usually should be obtained. In such a case, however, a knowledge of the technical concepts in this section will aid in dealing with the experts. Knowledge of this information will also prepare prosecutors for the possibility of the introduction of technical concepts by the defense in a trial.

Since the introduction of the first computer in 1944 (the IBM Mark I), computer technology has progressed at an astounding rate. Whereas the Mark 1 could perform 23-digit additions and subtractions in 0.3 second and could multiply 23-digit numbers in about 6 seconds, today's machines perform hundreds of thousands of such calculations per second. More important, today's computers are smaller, more reliable, and cost less than earlier computers. Consequently, computers are found in almost every aspect of our day-to-day lives. In addition to use in government, business, education, medicine, engineering, agriculture, scientific research, and communications, computers have become affordable for home use. Indeed, perhaps no other device invented by man has had such a profound and rapidly pervasive effect upon his society.

A. WHAT MAKES A COMPUTER WORK?

A computer needs two essential elements to process information: input data and a program. Input data are to be processed, and a program is a set of instructions that a computer is made to execute to process the data. Output is the processed data that will produce the desired end result only if the input data and program have been properly assembled and the equipment used has performed correctly.

After a program has been stored in the computer, data are fed through an input device to computer storage (alternatively referred to as main storage). The central processing unit, or CPU, controls the input and manipulates data according to the program instructions; the processed data, or output, are delivered from the desired computer output device(s).

The processing performed by the computer is usually of two types: arithmetic processing and symbol manipulation. Arithmetic processing uses equations in the form of a program and values supplied by input data for the variables in the equations. The computer determines the answer by adding, subtracting, multiplying, and dividing.

An example of symbol manipulation is to arrange a list of names in alphabetical order. To do this, the computer needs a program different from the one used to process arithmetic values because a different type of input is used and a different output is wanted.

Computers do only what they are instructed to do; they must follow a program. Accordingly, programming languages provide the communications link between the human and the machine. Hundreds of programming languages are in existence. Two of the most frequently used are FORTRAN and COBOL. FORTRAN is a language designed for scientific and engineering applications. Its acronym derives from "FORmula TRANslation", which is what it does best. COBOL, whose name is an acronym for "Common Business-Oriented Language", is more appropriate for computer business applications such as banking, payroll, order processing, bookkeeping and accounting, etc.

1. Data Structure

A computer cannot directly be instructed by English or any other verbal language the way a human can, but it can respond to coded information. Therefore, the structure of the information is essential. The coded instructions, or program, must conform to a precise coding scheme that the computer can be made to execute.

The computer can be made to record, process, and report data that are represented in verbal symbology provided that the symbols are translated into computer-usable form. Figure 2 illustrates how data flow from the input media, through the input device into the computer, and through the output devices onto the output media.

Data structures are arranged in a hierarchy, as shown in Figure 3. Data are made up of characters that combine into fields. Related fields make a record, and associated records form a file or data set.

A billing system is an example of a computer application. Based on sales slips, payment receipts, and outstanding balances, a card might be punched for each account showing the information in Table 23.

The characters that spell a name and identify a customer are a namefield. A complete deck of punched cards (records) for customers is a card file.

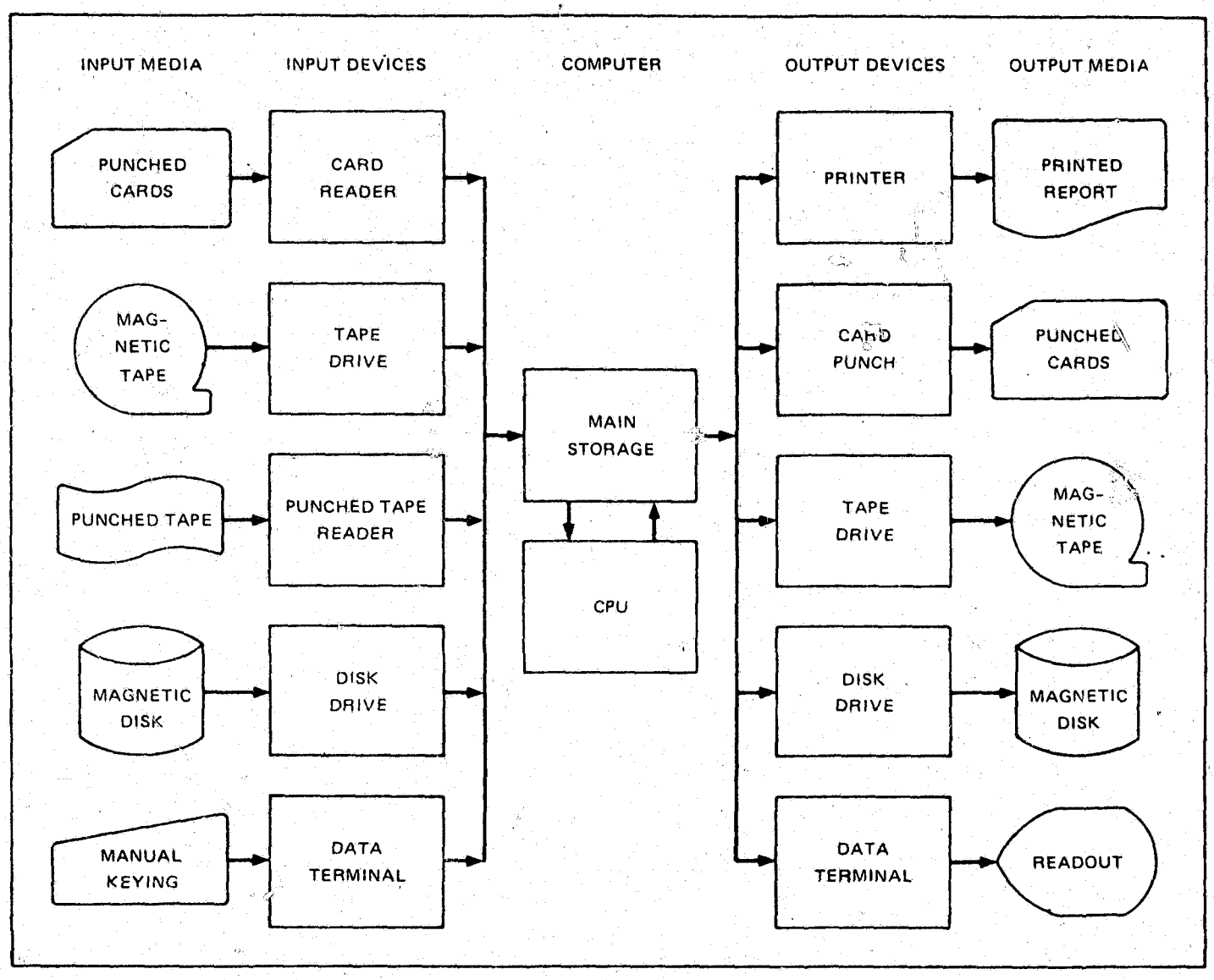


FIGURE 2 DATA FLOW

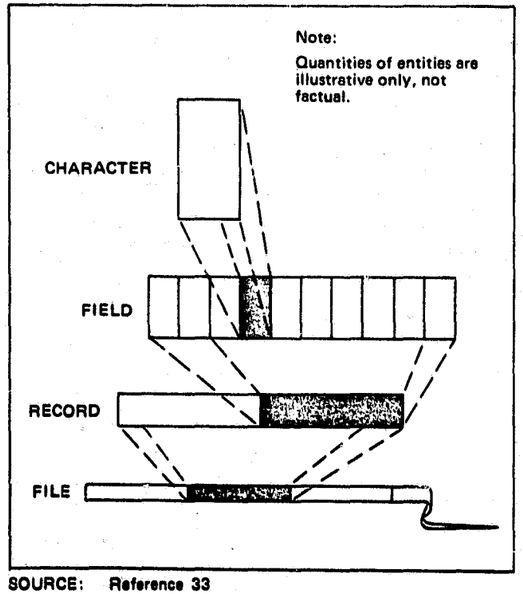
Table 23

MAKEUP OF TYPICAL DATA RECORD

Field*	Data	Example†
Name	Customer name	John Brown
Address	Customer address	123 Main Street "Anytown, CA 94001"
Old balance	Ending balance-previous month	$38.78
Charges	Items bought on credit during month	$16.50
Payment	Payments on account during month	$38.78

*Most businesses use account numbers, which constitute another field; this example disregards account numbers.

†Dollar signs, commas, and periods seldom are entered as input; the program inserts them.



SOURCE: Reference 33

FIGURE 3 DATA HIERARCHY

A program that has been translated into computer-readable language gives step by step instructions for the computer to follow in processing the information. For the system to work properly, data in each record and file must be in the sequence specified by the program.

2. Coded Input Data

One of the most common forms of input media is the key punched card. However, its use is rapidly being replaced by more modern forms, such as key-to-magnetic tape or disk. Nonetheless, the codes used in each are the same. Therefore, the illustration in Figure 4 uses the key punched card because it is a more visual medium than its more modern counterparts.

Figure 4 shows a common form of key punched card, and Figure 5 illustrates a card with holes punched for frequently used characters. The key punch machine punches the holes and prints the characters at the top of the card. To ensure that information will be arranged properly on the cards, it is first written on a data input form. Figure 6 shows one type of input form.

A prepared card file passes through a card reader, which reads each card and converts the punches into electronic signals, This is the form in which the computer uses the data internally. Processing depends on the binary (2-condition) representation of all data used by most digital computers; that is, either a signal exists or no signal exists. The computer translates that the absence of a signal is equal to the numeral 0 and that the presence of a signal is equal to the numeral 1. These digits, 0 and 1, are called binary digits, often contracted to "bit." They indicate the two states of a binary status and represent the data configuration inside a computer. (They have no correlation to rows zero and one on the punch card.) The holes in a punch card (or coded data or any other input media) are converted to different binary codes for different types of computers. It is the computer program that determines the internal form of the digits. Each number is represented by a unique sequence of bits. Characters or symbols are each represented by a set of bits in different patterns.

B. COMPUTER PROGRAMS

A computer program is a series of instructions or statements that directs the computer explicitly what to do with data to be processed so as to produce a certain result. Both the program and the data must be in binary-coded form compatible with the computer being used. Stored data, for example, will already be in the correct binary form. Input data will be translated to binary code as they are read. Output data will be changed from binary code electronic signals to holes in cards or paper tape, or magnetic patterns on magnetic tape or disk, or printable characters on paper, as required.

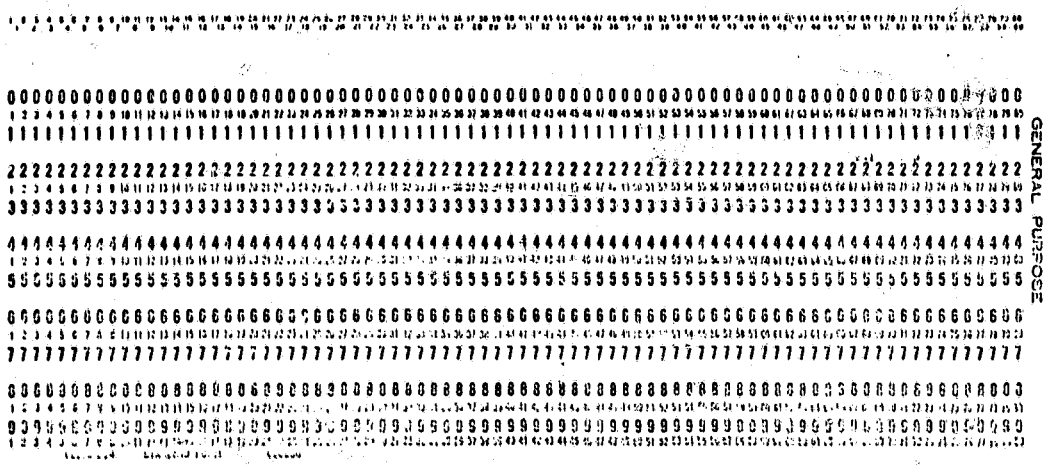


FIGURE 4 TYPICAL DATA PUNCH CARD

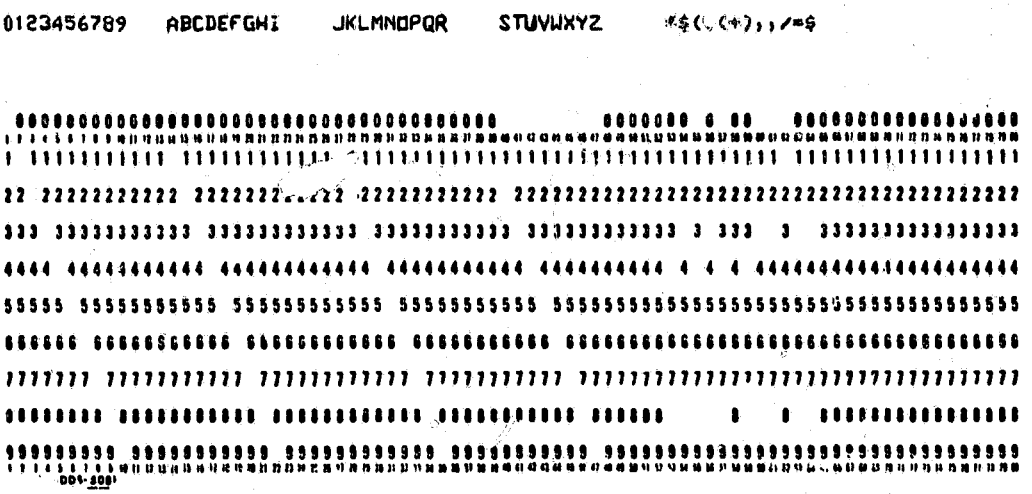


FIGURE 5 PUNCHED CARD WITH FREQUENTLY USED CHARACTERS

SRI

80-COLUMN CARD PUNCH LAYOUT

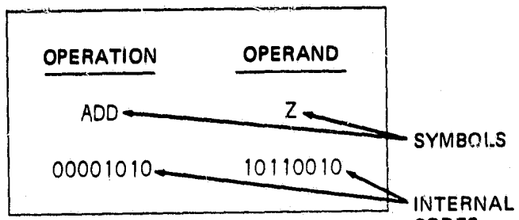
NAME	PROJECT NO.	PROJECT I.D.	PROJECT NAME	CARD PUNCH PRINT Yes ☒ No ☐	VERIFY Yes ☒ No ☐	DATE DUE OUT	SHEET
MARY JACKSON	P-110		ACCOUNTS RECEIVABLE			9/15/79	1 OF 1

```
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80
BROWN, JOHN                  123 MAIN ST                    ANYTOWN, CA 94001  3878  1650  3878
JONES MARY                   456 PARK PL                    ANYTOWN, CA 94002  5265  1840  5265
```

FIGURE 6 TYPICAL DATA INPUT FORM

In most computers, instruction makeup is referred to as single address instruction sets in which each instruction has two major parts: an operation (the action to be performed) and an operand, which is an address in storage or a constant. The operation describes what action the CPU is to take--for example, add, subtract, multiply, transfer control, shift, read, or write.. The operand identifies the memory location of the data to be processed or the data to be processed, depending on the type of command.

Figure 7 shows an instruction with the operation "add" and an operand "Z". The arbitrarily assigned, binary-coded instruction for "add" is 00001010, and symbolic address "Z" for the data to be added is at binary-coded location 10110010. The codes, although arbitrary here, have meaning to the computer.



SOURCE: Reference 33

FIGURE 7 A COMPUTER INSTRUCTION

Computer programs are often referred to as "software" to distinguish them from "hardware" that refers to computer equipment. A word of caution, however: These are jargon terms that have variable meaning and should not be used for legal purposes. Software sometimes refers to any computer program along with its documentation. Computer program documentation includes specifications, flow charts, I/O formats, test input data, sample output data, operating instructions, and program listings. A computer program of sufficient size is often organized into subprograms or subroutines, much as a book is organized into paragraphs and chapters. Further confusing the technology is "firmware" that describes a set of computing instructions resident in a special storage device and thought of as an integral part of computer circuitry.

The processing of data is done by a program containing instructions for reading data, for manipulating data in various ways, for deriving new data from old, and then for storing or writing data. Writing

includes the creation of new files (on cards and/or magnetic tape or disk) as well as printing.

Figure 8 shows one customer record, which constitutes input data, for the sample problem. The program executes the steps indicated in Figure 9 and flowcharted in Figure 10 to solve the problem. It reads and stores the characters in each of the card columns (fields) and then computes and writes the new balance. Starting with the old balance of $38.78, it adds charges of $16.50 to find a sum of $55.28. It then subtracts the payment of $38.78 to compute a new balance of $16.50. All that remains is to print a bill to show the customer's name, address, and new balance due. After this record has been processed, the program reads the next record and repeats precisely the same steps, using different input data.

1. Program Instructions

A computer processor does one and only one thing at a time. Instructions are processed one at a time. To make the processor's actions predictable to the programmer, computers are engineered to automatically perform the next instruction in working storage. The next instruction is defined as instruction beginning at the last working storage location of the just-completed instruction plus 1.

The programmer can override the processor's automatic next instruction assignment at any time. Special instructions known as transfers or branches provide this capability. The operands of these instructions contain the programmer-specified next instruction location. Typically, the computer processor has a built-in counter always containing the working storage location of the next instruction to be executed. The transfer or branch operations change the next instruction counter to the programmer-specified location contained in the operand of the transfer or branch instruction.

To perform data processing, the computer must have access to both the data and the set of instructions that cause it to perform its operations in a specified sequence. Therefore, computer programs contain both the instructions or procedures the computer is to follow and a definition of the data to be processed. There are several types of each, including:

- Instruction or procedure types: I/O operations, arithmetic, decision or conditional, editing instructions, logical operators, imperatives, and other.

- Data definition types: file definitions, constants, variables, and others.

Instructions consist of a symbol or character specifying the operation to be performed and the value or location of the operand or operands (that which is operated on).

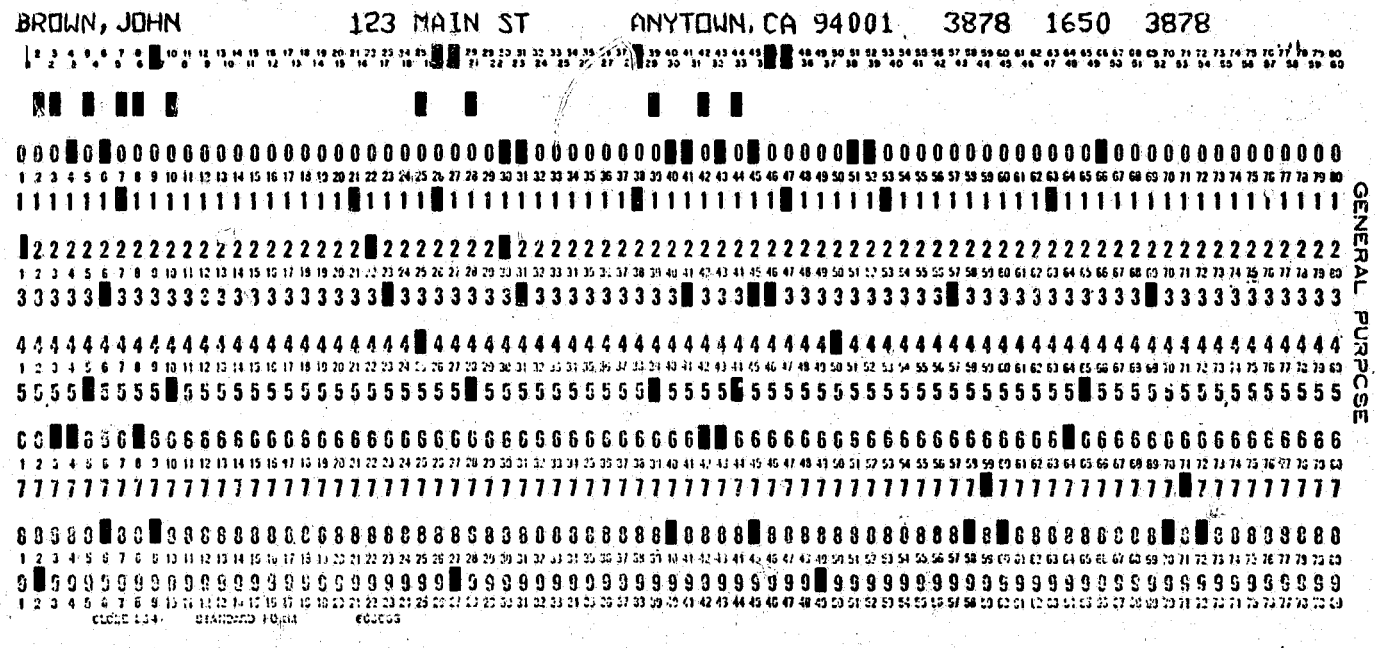


FIGURE 8 PUNCHED-CARD RECORD

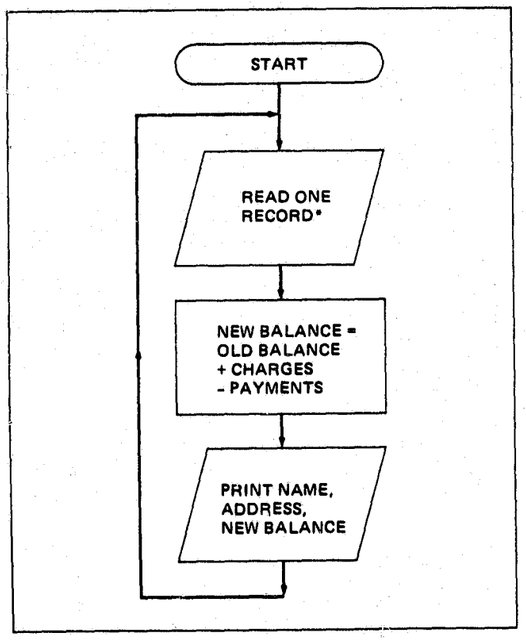
```
 10 READ N$, A$, B$
 20 DATA "JØHN BRØWN", "123 MAIN ST."
 30 DATA "ANYTOWN, CA. 94001"
 40 READ Ø, C, P
 50 DATA 38.78, 16.50, 38.78
 60 LET N = Ø + C - P
 70 PRINT N$
 80 PRINT A$
 90 PRINT B$
100 PRINT
110 PRINT, N
120 END
```

A$=first line of address
B$=second line of address
C =current month's charges
N =new balance

N$=customer's name
Ø =previous(old)balance
P =payments received

Note: A$, B$, C, N$, Ø, P are the fields in the input record. The program generates N in step 60. A print followed by a blank causes a blank line to occur on the printout.

FIGURE 9 SAMPLE PROGRAM



*Input record comprises name, address, old balance, charge, and payment fields.

SOURCE: Reference 33

FIGURE 10 ACCOUNTS RECEIVABLE SIMPLIFIED FLOWCHART

Input instructions cause data to be moved from connected storage devices such as magnetic disks, magnetic tapes, punched cards, and typewriter keyboards into a section of the computer's storage reserved for temporarily storing information that is now being worked on and for saving intermediate results. Output instructions move data from that same temporary or working storage to the connected storage devices, disks, tapes, etc.

Arithmetic instructions perform the fundamental operations of arithmetic: addition, subtraction, multiplication, and division, according to the rules of arithmetic. The values used in the calculations are obtained from working storage, and the results are usually stored in working storage.

Decision or conditional instructions determine the course of action the program is to follow next based on the results of a test of the conditions then existing. Data in working storage may be tested to determine whether it is greater or less than another value or a constant value, and the program will follow a different course of action if it is greater than if it is not.

Editing instructions modify the format of data in working storage to prepare for its use in output or in other instructions. Common examples include rounding, suppressing leading zeros, and insertion of special characters, such as dollar signs and carriage return (CR) signs.

Logical operators determine the course of action based on the terms expressed in the operation. The logical operators are AND, OR, AND NOT, and OR NOT. Logical operators and decisions/conditional instructions are often combined to test several conditions in one statement.

Imperative instructions specify an unconditional action to the computer such as DO X, STOP, etc. Common imperative instructions are MOVE, where data in one storage location are moved to another storage location specified in the instruction, and GO TO, where the processor proceeds to the instruction specified in the GO TO instruction to determine what to do next.

Other and miscellaneous instructions are available in most computer systems. These perform such operations as testing for end-of-data files, testing equipment readiness, reaching time clocks built into the computer, etc. The number and kind of these instructions vary with the design of the computer.

File definitions describe the content of the records in I/O data files. Each item of data in the record is assigned a beginning and ending location relative to the beginning of the record. Records are often grouped together on a data file and each I/O operation will transfer a group of records from or to the file. File definitions often define the number of records in each group.

Constants are defined fixed values or data items that do not change during the operation of the program.

Variables are defined data items whose values can be changed during the operation of the program. Variables are usually initiated, set to a beginning value, at the beginning of a program. That value is subject to modification by the program during the operation of the program.

2. Programming Techniques

Certain techniques have been developed that reduce the level of effort required to design, code, and debug programs. The more common techniques are used in most programs and are described here to further the reader's understanding of programming.

a. Loops

Certain sets of instructions are used repeatedly in most programs, whereas other sets are used less often or not at all. A typical payroll system paying 10,000 people may include the following instruction sets:

- Used for all employees

  A. Gross pay calculation
  B. Gross to net calculation
  C. Prepare earnings register

- Used for nonexempt employees only

  D. Verify overtime payments
  E. Calculate overtime pay

- Used for each payroll run

  F. Begin payroll run
  G. End payroll run

The following list indicates how the payroll might be programmed.

Program Step	Function Performed
1	F. Begin payroll run
2	Are there more employee records? If NO, go to step 11.
3	YES, get next employee record.

Program Step	Function Performed
4	Is this employee exempt? If YES, go to step 7.
5	D. Verify overtime payment
6	E. Calculate overtime pay
7	A. Gross pay calculation
8	B. Gross to net calculation
9	C. Prepare earnings register
10	Go to step 2.
11	G. End payroll run

This use of the loop from steps 2 to 10 allows the programmer to save considerable effort by writing each set of instructions only once instead of 10,000 times. In addition, he is able to use the basic pay calculation in routines A, B, and C whether or not there is overtime. This approach is called looping because the computer will circle (loop) from instruction step 2 to 10 and back until all employee records are processed.

Steps 3 through 10 are used conditionally if the answer to the question in step 2 is YES. This is known as a conditional loop. Frequently, programs will contain what is known as nested loops, where a loop within a loop will be repeated a number of times before the outer loop is completed once.

b. Tables

Programs frequently use sets of data items stored in working storage in the form of a table. The tables contain information that is referred to frequently in a program. A single computer program for an airline might use a point-to-point mileage and fare table and another table that converts the 3-digit airport code into the fully spelled out city and state name.

Tables are usually stored on a disk drive and are read into working storage when needed by the program. The program obtains information from the table by searching the table until it can match the data it is now working with with an entry in the table. For example, the airport code for Chicago is ORD and for Portland PDX. A flight record obtained from a data file could be converted as follows by using both tables:

Information	Data File	Report
Origin	ORD	Chicago, Illinois
Destination	PDX	Portland, Oregon
Mileage		1752.

c. Program Switches

It is often necessary to save the results of a conditional test for later use in a program. This is accomplished by setting a variable value that represents the test results. Payroll systems often use a switch to indicate whether this payroll process is the last for the quarter year and another to indicate whether it is the last for the full year. The program will perform the quarterly and annual procedures only when the switches contain the value indicating those calendar milestones have arrived.

There are several techniques for setting the switches and making certain they are correct. One widely used method requires the payroll department to enter a transaction record that contains key indicator information, such as "end of the quarter," "end of the year," etc. In other cases, the information is entered into a job set-up card in computer operations. This card is part of the setup that causes the payroll system to run.

d. Instruction Modification

As noted earlier, running programs are loaded into working storage along with the data. This allows the program instructions to be modified by other instructions and also permits data to be processed as instructions. When this occurs as a result of unplanned error, chaos follows but instruction modification is used deliberately to make programming easier.

A common example of instruction modification is found in conjunction with the use of subroutines. The program may transfer control to a subroutine from many places in the program. In each such case, the programmer will want to return control to the origin of the transfer when the subroutine is completed. This is accomplished by determining the desired returning storage address and loading it into the operand of the last instruction in the subroutine. That last subroutine instruction will not be equipped with an operand during source coding, but instead will receive one from other instructions during the running of the program.

e. Subroutines

A routine is a sequenced set of instructions that produces a particular result. These routines are generally or frequently useful and are segregated into what is known as a subroutine. Subroutines are designed to be used from anywhere in the program and are called on where and as needed. When the operations specified in the subroutine are completed, the program then returns to the main routine. Subroutines may themselves use other subroutines, etc.

f. Program Modularity

Most computer programs contain several hundred statements in their originally coded version. A compiler translates these several hundred statements into a greater number of machine language instructions, typically 500 to 1,000. Typically, programs of this size can be completed in 2 or 3 man-weeks, and one programmer does the programming work from beginning to end.

Programs of this size range have limited objectives and can be "read" and understood by a person familiar with the programming language used. However, programs of this type are nearly always part of a much larger system containing many such programs. To fully understand the significance of any one program, it is necessary to know what the previous and following programs do as well. For example, a prior program may alter the data being processed in unexpected ways, or a succeeding program may contain assumptions about the work performed in this program. This interdependency of programs in a large system makes it necessary to analyze the entire system before the role of any single program in the system can be understood.

Some computer programs are required to perform many tasks and may contain many thousands of computer instructions. These programs are usually broken down into discrete sets of instructions with an identifiable purpose. These sets are called modules. A system such as an airline reservation system contains many modules. Each program module can be programmed and tested by a different person, and large programs are designed in modular form so that several or many programmers can work on the program simultaneously. Development times and costs for programs of this size are measured in man-years and hundreds of thousands or millions of dollars.

Predictably, these programs are very complex, and highly qualified programming experts may spend weeks or months to gain an understanding of one phenomenon such as occasionally erratic results. Modularity was developed to allow the investigator to quickly narrow the possible sources of such a phenomona to a likely few, but modular design efforts are not always able to completely segregate the steps of each function into modules. Therefore, the search often leads from a likely module to another and seemingly unlikely module.

3. Programming Languages

Programming languages are designed to enable the human programmer to communicate more easily with the computer in a language more nearly like his own to cause it to perform specific operations in a defined sequence. These languages communicate with the computer via a machine language that the computer circuitry has been designed to recognize and respond to. Each computer model or model series has a different circuitry design, and therefore, machine languages differ from computer to computer. Programs in machine language are said to be in object code and are ready to load into the computer to perform processing.

The major types of programming languages, in addition to machine languages, are assembly languages, compiler languages, high-level languages, and specialized languages. A description of each type follows.

a. Machine Languages

Machine languages are coded as strings of zeros or ones that represent the binary ON or OFF condition. The computer is designed to interpret these machine language codes as instructions. Each instruction in the computer's internal instruction set activates certain parts of the processing circuitry, causing the desired process to happen.

Machine language can be coded by the programmer and is immediately ready for loading in the computer. Early programming was done in this manner: during the early 1950s computer programs consisted of thousands of zeros and ones representing characters of information, following one after the other without apparent reason or purpose.

b. Assembler Languages

Early experience with machine language programming demonstrated the need for an easier to learn and easier to use programming method. The first developments substituted character mnemonics (memory aids) for the sets of binary digits. Assembler languages use easily remembered symbols such as "A" for add, "S" for subtract, etc.

Programs coded in assembler languages must then be processed by a special computer program known as an assembler that translates the assembler language coding of the programs into the machine language coding used by the computer. The original program to be assembled is known as the "source code," and the machine language program output of the assembly process is known as the "object code." It is important to recognize that a computer program is a special-purpose file of data and can be processed like any other data in a computer.

Assembler language instructions have a one-for-one correspondence with machine language and therefore differ for each computer circuitry design. This makes it necessary to recode, reassemble, and test any assembly language program to make it run in another computer of different design. The expense and inconvenience of this program recoding and the rising cost of programming led to the development of the compiler and high-level languages.

c. Compiler Languages

Compiler languages perform the same and more functions than assembler languages do. Whereas in assembler programs each line in the source code becomes one-machine instruction, compiler languages are able to convert one line in the source code to one or many machine instructions. This translation is performed using a special computer program known as a compiler.

In addition, compiler languages are designed to match more closely the normal language of their intended user. In an example where one number is doubled then added to another, the programmer's source code might appear as follows:

	Code	Translation
Assembler code	L N/Z	Load N into storage location Z
	M Z/2	Multiply the number at location Z by 2
	A Z/X	Add the number at location Z to the number at location X
Engineering (high-level)	X = X + 2*N (= means replaced by) (* means multiplication)	Let the number at X become X plus twice the number at N
Business (high-level)	ADD NUMBER*(2) TO ANSWER	Add the value of NUMBER times 2 to the number at ANSWER

Note that the programmers coding in all three languages will convert to either the same machine instructions or their equivalent, and the same result will be obtained.

d. High-Level Languages

These are compiler languages that are also known as machine-independent. The design objective is to allow a program written in one of these languages to be used on different types of computers with few if any source coding changes required. Each type of computer has its own unique compiler that converts the high-level source coding as required by the machine language for that computer.

Most programming is now done with high-level compiler languages, of which the most common are:

COBOL	Common business-oriented language
RPG	Report program generator
BASIC	Beginners all-purpose symbol instruction code
FORTRAN	FORmula TRANslation
PL/1	Programming language/version 1
APL	A programming language

e. Specialized Languages

The flexibility of compilers has allowed the development of many specialized programming languages. One example is APT (automatically programmed tools), a widely used specialized language. The APT compiler converts source code developed by a specially trained programmer into a set of machine tool control instructions, usually on punched paper tape. These machine control instructions guide numerically controlled machine tools through the series of operations necessary to perform milling, bering, etc. Other high-level languages exist for systems simulations, report preparation, text editing, typesetting, and so on. Wherever sizable groups of programmers are coding computer programs to perform specialized functions that can be standardized, the opportunity and incentive exists to develop a specialized language that will improve their productivity. The suppliers who decide to sell computers or computer services to that market provide the necessary compilers to translate the specialized language into the machine language required by their computers.

C. COMPUTER SYSTEM STRUCTURE

1. Computing Equipment

The size and capacity of computers range from those of programmable pocket calculators that sell for less than $100 and home-use models that sell for a few thousand dollars to huge, super high-speed machines that

cost millions of dollars (see Figure 11). Between these extremes are computers designed for various purposes and with differing capabilities. The following examples show some of these differences.

A small computer may help to automate some applications for a small company--i.e., the accounting and payroll system--or to help in promotion mailings. Machines of this capacity are sometimes called minicomputers.

A computer with several high-speed input and output (I/O) units and a storage capacity of several hundred thousand characters could support the numerous processing tasks of a large brokerage firm. This could be considered a medium-sized system.

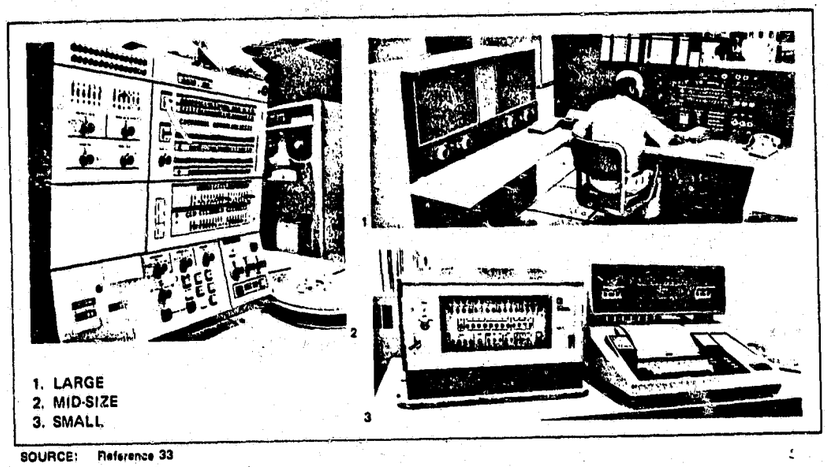
A large computer system often includes equipment costing millions of dollars, many high-speed I/O devices to handle several types of data, a huge storage capacity of billions of characters, several processing units handling different jobs at the same time, and perhaps even communicating processors that reside at different locations.

Regardless of size, capacity, and location, the hardware components of any computer system include I/O devices, storage devices for internal and auxiliary storage, and the CPU. The functional characteristics of these components are as follows:

- Input devices--move data and programs into the system.
- Output devices--move data from the system, or record instructions or data for recycling input back to the system.
- Storage devices--store the programs and data to be used by the system.
- Processing and control devices--execute the programs to perform logic and arithmetic and manipulate and move data within the system.

Several types of I/O devices may be used with a computer system. Some perform only input or output functions. Some perform both input and output; and some have input, output, and storage functions.

One of the most common input devices used is the card reader, shown in Figure 12. The card reader performs the input function by sensing the holes punched in a card and emitting electrical signals to the computer, based on the position of the holes, to indicate certain characters or numerals.



1. LARGE
2. MID-SIZE
3. SMALL

SOURCE: Reference 33

FIGURE 11 COMPUTERS OF VARIOUS SIZES

SOURCE: Reference 33

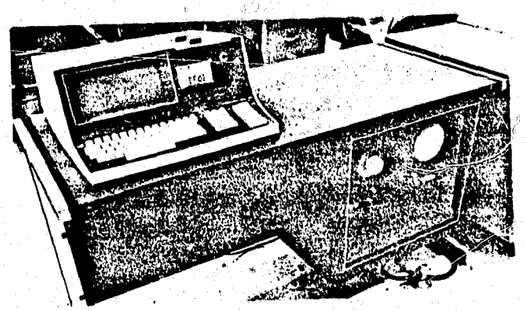
FIGURE 12 CARD READER

A similar input device is used for key-to-disk or key-to-tape input. An operator at a terminal keys the information through a conversion system directly to disk or tape storage (see Figure 13).

Other types of input devices are optical character readers (OCR), magnetic ink character readers (MICR), and point-of-sale (POS) terminals. An embossed charge card, for example, is designed for optical character recognition as are special pencil marks in predetermined positions on a card or paper used for multiple choice examinations. The use of MICR has become common in banks to process checks and other documents automatically; whereas, POS terminals (see Figure 14) have been effectively used in retail establishments to record transactions by using a keyboard or sensors (sensing wands) attached to a terminal to read data from the tags (Universal Product Code) on the product being sold.

Output devices include the card punch, tape punch, and printer that are used to transfer data out of the computer into the medium used with each device; i.e., cards, paper tape, paper forms, etc. (See Figures 15, 16, and 17.) Another output only device is the computer-output microfiche or microfilm (COM) recorder. The data from the computer are recorded on photosensitive film in microscopic form. Therefore, data can be printed in more concentrated form than with standard printed output. However, to be retrieved, the data must be read through a microfilm reader.

Some examples of devices that can be used for both input and output are: the control console (see Figure 18), a device containing the controls and indicators that allow communication between the computer system and operator. The operator uses the console to start and stop the system, receive instructions and status information, control some of its operations, and insert special instructions or data, i.e., to provide I/O. Similarly, cathode-ray-tube (CRT) terminals and hardcopy terminals (such as the teletype terminal) provide input to or output from the computer. All of these devices use keyboards to key data into the computer. For the CRT, output from the computer is printed on a television-like screen (see Figure 19), whereas output provided by a hardcopy terminal is printed on paper. Magnetic tape, disk, diskette, cassette, and drum devices may be used both for I/O.

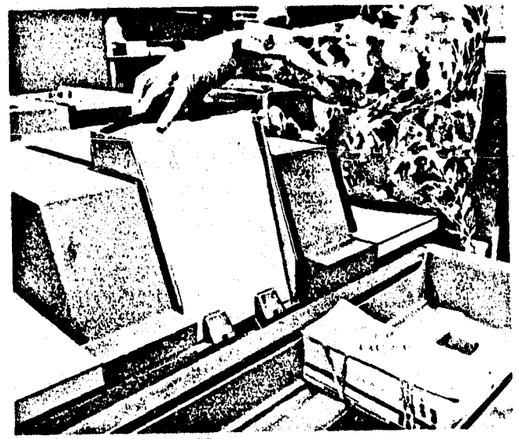


SOURCE: Reference 33

FIGURE 13 KEY-TO-TAPE OPERATION

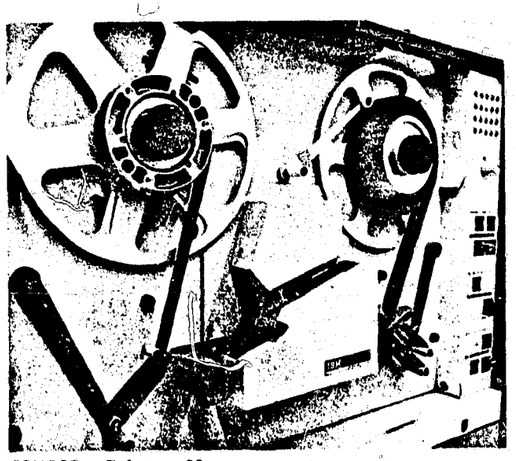
SOURCE: Reference 33

FIGURE 14 POINT-OF-SALE TERMINAL



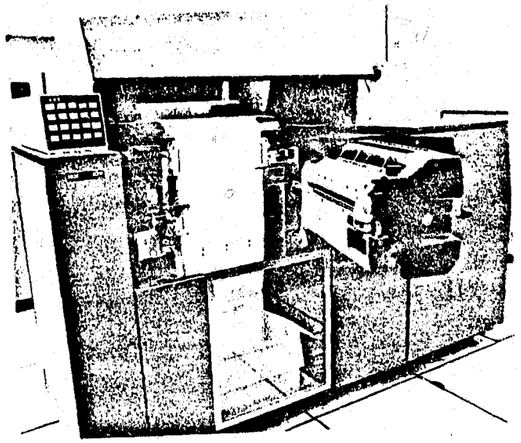
SOURCE: Reference 33

FIGURE 15 CARD PUNCH



SOURCE: Reference 33

FIGURE 16 PAPER TAPE PUNCH



SOURCE: Reference 33

FIGURE 17 LINE PRINTER

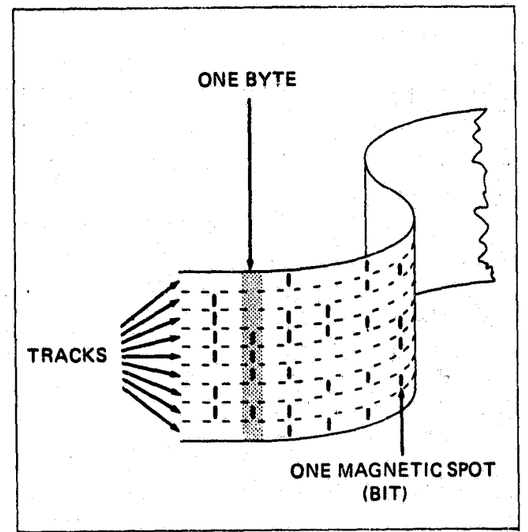
SOURCE: Reference 33

FIGURE 18 CONTROL CONSOLE

SOURCE: Reference 33

FIGURE 19 CATHODE-RAY-TUBE TERMINAL

High-speed data storage devices retain data and programs during processing. Other names that are frequently applied to the principal storage unit in a computer system are main storage, central storage, or core storage. Auxiliary, secondary, or peripheral storage in the form of magnetic tapes, disks, drums, diskettes, or cassettes expands the storage capacity of a system but has far slower access time. Data stored on tape coated with a ferromagnetic material are in the form of tiny invisible magnetized areas that are sensed electronically. A magnetized spot represents the binary digit 1 and an unmagnetized spot represents 0. The diagram in Figure 20 illustrates coding of data on a magnetic tape. The use of magnetized or unmagnetized spots represent the same binary digits on tapes, disks, drums, diskettes and/or cassettes. When a program is too large to fit in main storage, it can be put in auxiliary storage to be recalled in segments during processing. Programs are usually segmented into subprograms. Typically, all data pass through main storage on their way to or from the CPU, I/O devices, and auxiliary storage. Data and instructions in main storage consist of individual bits stored electronically in a predetermined coding scheme. Groups of bits are known as bytes or words. Storage is like a set of mailboxes, with each box having an address. Each instruction occupies one or more words. When a program is written and stored, its instructions occur one after another in sequence so that processing will be orderly. Data and instructions are placed in storage in the same way; in fact, instructions in a program



SOURCE: Reference 33

FIGURE 20 DATA STORED ON MAGNETIC TAPE

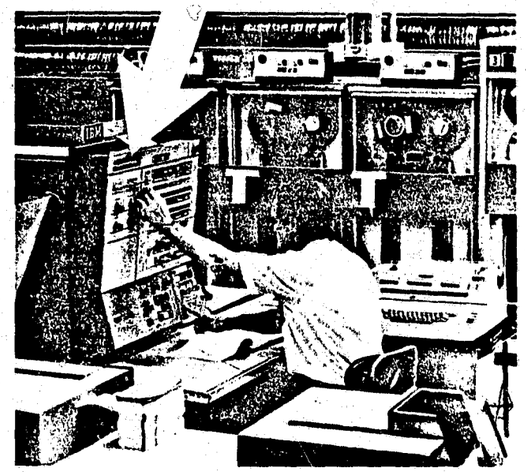
are a form of data. A data word can be used as an instruction. If its bit pattern satisfies the requirements of a valid instruction, an operation will be performed. If the data are invalid as an instruction, the program probably will halt, and the computer operator should receive a message on the console about the event.

The CPU performs the data processing functions as directed by a program. It also controls the movement of instructions and data within the system. The CPU usually has two functional sections: a control section and arithmetic-logic section. It also has registers that are designed to temporarily store data, arithmetic and logical operands, results, and instructions to be processed. A photograph of a CPU is shown in Figure 21.

The control section directs the I/O devices, decodes and executes instructions, and routes data between storage and the registers and arithmetic-logic unit. It is the director of the entire system.

The arithmetic-logic section contains the circuits that perform arithmetic and logical functions.

Registers are small storage areas that temporarily hold data during processing. For example they hold the address for a particular item of data, an operand, or the operation code portion of an instruction to be executed.



SOURCE: Reference 33

FIGURE 21 CENTRAL PROCESSING UNIT: ARITHMETIC LOGIC SECTION

2. Computer Operating System Functions

A computer operating system includes all the computer programs necessary to operate a computer. Types of programs include: compilers and assemblers, utility programs, and control programs for operating the system.

Generally, an operating system consists of an executive control program and a number of processors. Each processor performs a specific function upon command of a control statement provided by the operator or application program. The function of each processor can usually be considered either of the job management, data management, or task management type. A list of some major operating system functions, according to type, is given below.

- o Job management
  - Job scheduling: read and interpret the control cards, allocate computer time, form job queues, handle priorities, load programs, and respond to traps and interrupts.
  - I/O allocation and control: dynamically match and assign I/O channels and devices with job requirements, monitor their status, and control their operation.

- Operator communication: handle all communications to and from the operator.

- Error, diagnostic, and recovery processes: discover errors, issue diagnostic messages, and handle system recovery procedures.

- Utility and miscellaneous services: handle special I/O considerations, intercommunication between terminals, security, sharing of data base considerations, and device to device transfers.

o Data management

- File control: describe a file, input data into the file, maintain the file.

- Open/close files: open (make available for use) and close files as required by a specific task.

- I/O supervision: control the movement of data between elements of storage.

o Task management

- Task supervision: load the task (a unit part of a program) into main memory for execution, and control the movement of tasks between primary and secondary storage.

- Interrupt handling: handle all interrupts to the execution stream.

- Facility and user time accounting: handle accounting of user and system program execution time and of system component use time.

- Language translation: provide capabilities to assemble or compile source language programs.

The objectives that an operating system must meet for a user's job or run are: automate the steps in a job-to-job transition and in the setting up of a specific job; accommodate an environment of diverse applications and operating modes; reduce total job time and increase efficiency; provide necessary diagnostic aids; and increase programmer productivity.

Operating systems are usually supplied by the computer manufacturer and can be as large as 5 or 6 million instructions requiring several thousand man-years to design and develop. They are probably the most complex products of human endeavors. Programming must still be

considered a cottage craft or art that is only recently being transformed into an engineering discipline. A computer operating system for a large computer is not predictable because it is so complex; its performance under all conditions is not known and could never be considered to be perfect according to a given set of specifications. Errors or bugs in operating systems are discovered throughout their lifetimes, and correction of discovered bugs frequently introduces new bugs or deviations from specifications. Any large computer programs suffer from these problems. They need continual maintenance just like a complex machine does--not because they wear, but because of the discovery of bugs.

Operating systems function in two modes, batch and on-line. These are described in the next two sections.

3. Batch Operating Systems

Many business activities occur periodically rather than constantly. The hourly worker is paid for his work weekly, or semimonthly, or on some other pay-period basis. The time records that he/she turns in during the pay period are gathered into a batch, along with the time records of all others on the same payroll. This batch of time records is then processed in a batch, payments are made, and year to date records brought up to date in one large batch and on a scheduled date.

Most computer systems are used in batch mode. Banks use batch mode to process checks, credit or debit the proper accounts, produce no sufficient funds warnings, produce monthly statements, etc. Retailers use batch mode to record purchases and on a scheduled date to calculate finance charges and produce monthly statements for mailing. Batch is usually the most economical way to provide periodic processing and when it is not necessary for the systems records to contain or reflect all information up to the latest minute or hour.

a. Input Handling

Input for a batch mode is collected during the period between processing runs. For example, weekly time cards for hourly employees are usually gathered from the time card racks once a week and submitted to the computer in a batch. If the worker is paid every two weeks, the payroll processing is done with two weekly batches of time cards. In another case, the employee may be clocking into a clock that automatically records the time, date, and employee number onto a data processing recording device. Again these data are submitted to the computer in a batch, perhaps at the end of each day.

These batches of employee time clock records are called transactions. The first step in handling transactions is to convert them to a computer-processible form. Time cards go through a data entry process that records the information onto a computer input medium, such

as punched card, magnetic tape, or magnetic disk. The converted time card records then become the payroll transaction file.

Typically, the payroll transaction file is sent first to a batch computer system that edits or checks for errors. The editing may, for instance, determine that each employee number in the transaction file is for a currently active employee, that no employee overtime is reported without proper authorization, that one and only one time card exists for each current employee, and so on. The edit system produces a new payroll transaction file containing only the correct records and also produces a list of time records rejected for real or possible error. The rejected records are then corrected and entered again through the edit system. This process is continued until the person responsible for payroll decides the computer input transactions are free of error.

b. Processing and File Handling

When the time record input transaction file has been edited, corrected, and cleared for use, the payroll process itself occurs. The time record for each employee is placed in the current hours space in the employee record, the gross and net pay is calculated and the various outputs, including paychecks, are prepared. Proccessing occurs at computer speed and several thousand payroll calculations can be done each minute. Table 24 illustrates the files that might be used in and produced by our simplified payroll example.

The previous payroll master file was produced as output from the last weekly payroll process. The payroll master file output from this week's process will in turn become the input to next week's payroll. In this way, the constantly changing year to date records are kept current.

The payroll master file also contains less variable and static information such as social security number and hourly pay rate. To change static information such as the pay rate, a transaction is entered into a separate process--usually called the master update. New employees are added, names are revised, and other changes are made to the payroll master as in the update process. Typically, every computer file passes through one or more update systems during each processing cycle so as to provide the opportunity to change both the static and constantly changing information.

We have discussed a transaction file, an input master file, and output master file. Batch processes also produce output files such as the check file in the example. The check file can be used for other purposes in addition to printing the paychecks. It may, for example, be used to produce a check register in social security number sequence. This is accomplished in the payroll system by sorting the file in the computer to the desired sequence and then printing the required report.

Typically, payroll processes are done on sequence, one employee at a time. This approach is used because all or most of the employees have

Table 24

EXAMPLE OF A SIMPLIFIED PAYROLL FILE

Information Description	Input		Output	
	Time Record	Previous Payroll Master File	New Payroll Master File	Check File
Name	Joe Smith	Joe Smith	Joe Smith	Joe Smith
Number	101142	101142	101142	
Hours Worked	41	38	41	
S.S. number		363-99-9999	363-99-9999	363-99-9999
Pay rate (dollars)		5.50	5.50	
Year to date				
Gross earnings		2,113.55	2,341.30	
Taxes		304.04	342.21	
Net earnings		1,809.51	1,999.09	
Weekly				
Gross earnings		209.00	227.75	
Taxes		36.11	38.17	
Net earnings		172.89	189.58	189.58

time record transactions each pay period. In the above example, the two input files would be arranged in the same sequence, probably employee number, and processed together. These kinds of sequential files are usually kept on magnetic tapes.

It is also possible to use direct-access techniques that store and retrieve information at random as directed by the computer program. Computer disk drives are devices that allow access directly to any individual record as directed by the program. Files on disk drives can also be read and processed sequentially. In our example, the payroll master might be kept on a disk and updated directly when a few rate changes are made, but it can be retrieved and processed sequentially when the entire file is used to process the payroll.

The discussion thus far has centered on a process that updates one master file at a time. Many systems are designed to update at one time several files with the transactions. For example, the time-record transaction file can also be used to update a separate file that is keeping track of total hours worked and is not concerned with dollars. This hours file also may be either a sequential or a direct-access file.

c. Output Handling

The payroll example given earlier in this section will produce several outputs, including such items as:

- o Files
  - New Payroll Master File
  - Check File
- o Reports
  - Pay Checks
  - Check Registers
  - Tax Reports.

Each output must be distributed in a prescribed fashion. The output files will be given to the person responsible for the computer center data files. This person is usually called the librarian. The librarian records the date, volume number, name and number, and other vital information and stores the file so it can be retrieved when next needed.

The reports will be printed, burst apart, and sent via courier or mail to the proper recipients. Other reports such as the Check Register, might be microfilmed and the film sent to the recipients by the same route.

d. Local and Remote

The payroll example cited earlier involved three main groups, the employees, the payroll department, and the computer operation. These groups may be physically near to or far removed from each other. When they are physically adjacent, the process is known as local or centralized processing, and when they are physically removed, it is known as remote or distributed processing.

Whereas local processes rely on couriers, mail deliveries, etc. to move information, remote processes sometimes must rely on data communications circuits to move the information over the distances among the groups. Remote processing systems typically differ from local processing systems in these ways:

- o Input preparation is near the employees and may be separated from the computer processing center.
- o Output preparation, printing, and bursting are near the payroll department and may be separated from the computer processing center.
- o The systems contain additional checks and edits to make certain the I/O data are correctly transmitted.

Facilities that are dependent on a distant computer linked by communication circuit are equipped to perform at least part of their own data processing work. Typically, they have data entry equipment that allows them, for example, to convert time records into computer-readable input transactions and also often have printing equipment that can produce output checks, check registers, etc. The I/O equipment connects to a data communication circuit directly or through specialized communications equipment.

In other cases, the I/O equipment includes a computer. This approach allows the remote facility to do at least part of the processing. Transaction input is partially edited and corrected at the point of entry before it is communicated to the computer center for processing. However, it is not possible to completely edit the time-card transactions unless the payroll master is also available, which usually means the final edits occur during the payroll process in the computer center.

4. Real-Time, On-line, and Time-Sharing Systems

Real-time systems are designed to perform their processes at the speed with which events occur. For example, the airline reservation file must be instantly changed when the clerk enters the necessary information. Any other clerk attempting to reserve the same seat even a fraction of a second later must be advised it is not available. Real-time system users such as reservation clerks are connected directly to

the computer through a cable or data communication circuit. This allows them to send information to the computer as events, sales, cancellations, etc. occur and to determine the current status of the files at any time through a procedure known as inquiry.

On-line systems users are also connected directly to the processing computer and enter activity information as it occurs. However, on-line systems are not necessarily designed to update the information files as transaction information is received. Airlines, for example, may enter their employee time records on the reservation clerk's equipment. The on-line system receiving the payroll transactions would store them on a payroll transaction file in the computer. This transaction file would then become the input to the batch payroll system at the end of the pay period. The airline might decide to design their payroll information collection system in this way to avoid buying special equipment for entering payroll information and/or to provide daily reports of hours worked by location.

Real-time system data files are at all times kept up to date and accessible to the system. Direct access devices, such as disks, are used on real-time systems to allow the system to access the files in the random order in which access requests are received from the users. Therefore, real-time system master files are found on disk drives connected to the system during the time the system is in operation.

On-line system users also need immediate and random access to the data files, but do not necessarily need to immediately update the files. Therefore, the data files are found on disks, but the data may not reflect the most recent changes.

Time-sharing is a technique that permits more than one real-time or on-line system user to share the same computer simultaneously. The number of simultaneous users is limited only by the size of the computer. The computer serves time-sharing users one by one, but allows each one only a brief processing time. Thus, in a time-sharing system designed for a limit of 50 users, each might be limited to 1/20th of a second. This means that no one user would have to wait more than 2.5 seconds for service. Because humans take several seconds to act or react, most users of such a system would receive a fast response and have the impression they were the only users. Examples of use of three commercial time-sharing services are presented in Appendix D.

a. Input Handling

Most input is submitted directly to real-time, on-line, and time-sharing systems. The batching of input documents and the data conversion steps found in batch systems are both avoided. Instead, the person who is conducting the activity nearly always enters each transaction into the system as it occurs. These persons are equipped with a terminal device, such as a keyboard, to enter the necessary data. Real-time, on-line, and time-sharing systems are designed to cause the

computer to periodically interrogate each connected device to determine whether it has information ready to send. This interrogation process is often called "polling."

When an affirmative response is received indicating a terminal is ready to send data, the system initiates the actual transmission of the information from the terminal device to the computer. At the end of the data transmission, the system may be, and usually is, designed to send an acknowledgment back to the sending device. This technique assures the person sending the information that the computer correctly received it.

Immediately following receipt of the information at the computer, the following tasks are usually performed:

- Record the information onto a transaction file called a log. The date and time and the source device are also usually recorded on the transaction log.
- Edit the transaction to make certain it is acceptable. Dates and times must be numeric, names alphabetic, and everything in the transaction must be in a specified sequence, etc.
- Reject the unintelligible transactions, indicating the reason for rejection to the sending device by an error message such as, "NAME MISSING," "ACCOUNT NUMBER INCORRECT," etc.

Subsequently, the system performs the required operations on the transaction. There may be one or many types of transactions, each requiring its own unique handling. The transaction type is often defined by an identifying code in the transaction. In other instances, the connected devices are designed or designated to send only one type of transaction, and the system determines the type of transaction by identifying the device.

An airline reservation system must be able to handle many types of transactions. A partial and simplified sample of the possible types of transactions might include:

Transaction Code	Possible Handling
INQ (Inquiry) XX	Find the flight record referred to in XX and transmit the information on file regarding that flight to the inquiring device for printing or display.
RES (Make Reservation) XX YY-YY	Reserve a seat for the person named YY-YY on flight number XX.

Transaction Cod/	Possible Handling
INQ (Inquiry) XX	Find the flight record referred to in XX and transmit the information on file
DEL(Cancel Reservation)XX YY-YY	Release the seat on flight number XX reserved for the person named YY-YY and make it available for use by another party.
ADD (Add a Flight) XX ZZ-ZZ	Add a flight number XX according to the information in ZZ-ZZ.
SUb (Delete a Flight) XX ZZ-ZZ	Delete the leg or legs of flight XX specified in ZZ-ZZ and produce a list of the customers holding reservations that need to be notified.

Note that the INQ, RES, and DEL transactions would be the normal everyday business of the reservation clerk. However, reservation personnel do not add or delete flights and therefore do not need to be authorized to use the ADD and SUB transactions. The use of the ADD and SUB transactions would be limited to designated authorized parties, such as flight operations personnel. To prevent any party from using transactions that are intended for another, several techniques are available, including limiting the entry of these transactions to certain physical devices and/or requiring the entering party to identify himself by preceding his transaction entry with a special code called a password.

Real-time, on-line, and time-sharing systems also receive a part of their data from batch processes. Often, 24-hour-a-day systems, such as airline reservations systems, are fully stopped once each day. This period when the system is not operating is used to perform several batch systems functions, including:

- o The file of connected terminal devices and flight schedules is changed by loading in a new batch of data identifying the terminals and flights that will be available during the next 24 hours.
- o The transaction log is terminated, removed from the computer, and stored in a safe place such as a fireproof vault.
- o The system master files are copied, and the copy is removed from the computer and stored in a safe place.

b. File Handling

On-line, real-time, and time-sharing systems contain several types of files, including:

- o Reference files containing basic information the system needs to operate, including the identification of system users and devices accessing the system. These files are used frequently and are usually stored in the computer for fast access.
- o A log file recording all transaction inputs sequentially as they occur, usually on a magnetic tape drive.
- o A master file, usually on a direct-access disk drive, that contains the data being used and updated by the system user.

These files are often called the system's "data base." Data base is a term usually used to describe files that are the central and often sole source of information that is needed and used by various parts of the organization. Numerous vendors market what are called Data Base Management Systems (DBMS) that are designed to reduce the time and expense required to design and develop on-line systems.

As noted earlier, the reference files are loaded into the system periodically, often when the system is started up at the beginning of a processing period, such as a day. Certain changes may occur during the period that affect the reference files. For example, a terminal device may fail, and the system will be unable to send or receive information to that device. On-line systems are usually designed to shut down the failing device and notify computer operations personnel. The shutdown is accomplished by annotating the reference file of terminal devices to indicate a certain one is inoperable. The system will then no longer poll the inoperable device to determine whether it is ready to send or receive information. When the problem has been corrected, computer operations personnel enter a special transaction that restores the device to the polling sequence by removing the inoperable annotation from the reference file.

Recovery and Restarts -- The transaction log file produced by the system is a record containing all transaction information entered and other identifying information, including time and place of origin. The log file is a valuable source for volume statistics, but its primary purpose is to permit the system to recover after a failure that destroys the current master files or makes them inaccessible to the system. When that situation develops, it is not possible to proceed until the master files have been restored to their correct status just prior to the failure. Therefore, the system's users are not allowed to access and use the system until it is operating with correct information.

The restoration of service is accomplished by executing a computer program that recovers all the necessary information. The copy of the master file as of the beginning of the processing period and the transaction log for the period are inputs to the recovery program that repeats all the transaction processing up to the point of failure without, however, sending output information to the terminal devices

again. The primary outputs of the recovery program are the reconstructed master files that allow the system to be restarted at the point of failure, once again allowing the users to access the system.

These recovery processes are time-consuming, and in many such systems it is essential to keep the system operational all or nearly all of the time. Airline reservation clerks are nearly helpless when their reservation system is inoperable, and customers may and do go to another airline that is able to immediately reserve a seat on a competitive flight. Various techniques are used to reduce recovery times to the shortest feasible interval, including saving transaction log and master file copies about every hour to reduce the amount of processing necessary to restore the master files. When it is economically feasible, the entire system is duplicated on a standby computer that is ready, complete with separate copies of the current files, to take over system processing if anything goes wrong on the primary computer.

Design Alternatives -- The master files are often the focus of real-time, on-line, and time-sharing systems. The systems are designed to keep these files up to date and to extract the information from the master files as required to support the system user's needs. The airline reservation system keeps the reservation file up to date to the last transaction. This is essential because it may receive another request for the same seat within seconds.

Credit card companys are less precise in updating transactions. Instead, they normally update their customer master files at night in relatively inexpensive batch mode. These companys mail customer charge slips and payments to the computer center. This means the most recent several days' transactions are not reflected on their files. Nonetheless, they maintain on-line systems that allow the users to access the credit card customer files to determine that the account is valid and that a customer's new purchase will not exceed the credit limit. These are not real-time systems because the master files are not kept current.

The credit card companys undoubtedly prefer the capability to charge the customer's account immediately after each purchase. This would allow them to detect and immediately reject over-limit purchases and to guard against "shopping sprees" by the criminal who has just gotten possession of the card. However, immediate updating would require the connection of each sales station to the computer by a communication circuit and necessitate larger and more expensive computers. The additional costs to convert the credit card on-line systems to real-time systems are apparently not justified by the risks associated with loss or theft of their customers' credit cards.

The long-term trend is toward real-time and away from on-line modes for most systems, including credit card control systems. Real-time credit systems are now appearing in retail chain operations where one

machine does double duty as both the cash register and on-line computer terminal and where the number and therefore cost of communications circuits is minimal.

Updating Techniques -- Two approaches known as memo-update and update-in-place are used to keep files up to date at all times in real-time systems. Memo-update systems do not actually change the information on the system master files. Instead, the transaction information is stored in a separate file when it is received at the computer, and the master file is annotated to indicate that a change has occurred and often where the change can be found in computer storage. If a second transaction is received, another annotation is made--usually in the first transaction record in storage. In a credit card example, the files might then be as shown in Table 25.

Table 25

EXAMPLE OF A CREDIT CARD MEMO-UPDATE FILE

	Master File	Transaction 1	Transaction 2
Storage Location	1114212	3014020	3020117
Customer name	Joe Smith		
Account number	59-83770-212	59-83770-212	59-83770-212
Amount purchased		59.86	79.99
Credit limit	1000		
Amount owed	814.32		
Credit remaining	185.68		
Annotation of transaction Storage location	3014020	3020117	

This structure allows the system to determine at any time the total amount Joe Smith owes and his remaining credit. For example, the sales clerk handling Transaction 2 would enter the amount of the new sale. The system would locate the appropriate master record, validate the card account number, and determine that the purchaser is within the credit limit: \$185.68 - (\$59.86 + \$79.99) = \$45.83 credit remaining. The system may be designed to take a variety of actions in addition to authorizing the sale and posting the transaction. It might, for example, notify the sales clerk that the customer is nearing his credit

limit, and the customer should be asked to visit the credit department if he wishes to increase his credit limit. Or, it might be designed to supply the clerk with the credit remaining information along with instructions to so advise the customer.

Memo-posting systems require a batch system that is used periodically to create a new and up to date master file and to eliminate the annotations. In credit card applications, these batch systems are run at night when the on-line system is idle. Credit card batch systems also record the transactions onto a log file and save them for inclusion in the next monthly customer statement. In the example, if Joe Smith's statement cycle were to occur that same night, then the two memo posted transactions would appear on his statement and be included in the amount calculations.

Update-in-place, real-time systems perform the same functions and provide the same capabilities. The design approach is different. The master file is updated each time a transaction is received and no annotation is necessary. However, it is still necessary to keep a record of the transactions, not only for the eventual production of the customer's statement, but also for the restoration of the master file if it should be destroyed during the day's operation through computer operator error, equipment malfunction, or other failure. The update-in-place and memo-update approaches are sometimes used together in a system, with some files handled one way and other files handled the other way.

c. Output Handling

Batch systems often produce large printed or microfilmed reports. These reports can be stored by the user and retrieved for reference purposes when necessary. The lookup time, especially on printed reports, can be substantial. On-line systems can be designed to produce these same reports, but more often they are designed such that the computer does the lookup in its storage and provides the user with the information he needs and no more. The airline customer's interest is limited to his own travel routing and the reservations clerk serving him usually need look no further to accommodate his needs. Thus, the reservation clerk requests and gets information on the 130 seats on one flight, not the many thousands of additional seats that may also be available in the airline system.

On-line, real-time output is often produced in the form of displays on a screen. This display might contain, for example, the unassigned seats on Flight 83 bound for Duluth, or John Jones credit limit and unused credit amount. The display content is designed to meet the specific need of the requester, and the requester defines his need to the system by entering a specified type of transaction that he knows will provide the information required.

Display information can also be printed if a printer is available. Printers are mechanical and often much slower than display units of the same cost. They are used sparingly if at all in most on-line systems. However, there are on-line systems for the primary purpose of providing printed reports. The most common are message systems that move or switch typewritten information entered at one location to one or more other locations at electronic speeds. Most message-switching systems now use a computer to receive, validate, and dispatch the messages. Message systems usually do not have a master file, but otherwise are similar in design to other on-line systems.

Confidential or sensitive information printed by a computer batch system is safeguarded by limiting access to the printed report, often by locking it up when it is unattended. Many on-line systems can also print confidential information in many locations at once. This makes each user with access to the on-line system a guardian of the information he receives, thereby creating a situation that is difficult or nearly impossible to control. Therefore, confidential and sensitive information is usually made available to only a few individuals who are authorized to receive it and are issued a special password known only to them and the computer; the terminal they use may also be located in a secure area. There are many variations and approaches to the on-line security problem, but none has been completely successful.

5. Process Monitoring and Control Systems

Process monitoring and control real-time systems are computer systems used to measure and control external processes and operations. In many cases, the systems measure one or more current conditions with respect to limits programmed into the system, and they feed back signals that adjust the operation to keep those conditions within the limits. These feedback or "closed loop" systems are called process control systems. In other cases, there is no feedback; instead, the system only reports and records out-of-limit situations. These are process monitoring systems.

a. Inputs and Outputs

Process monitoring and control systems are designed to control physical, nuclear, electrical, or chemical processes, through electronic devices connected through a circuit to the computer. Typically these devices consist of limit switches, photocells, scales, thermometers, etc. These input devices measure the variables constantly and over an infinite range of values. These are called analog measurements. These analog input signals are converted to digital values by an "analog to digital converter" placed on the circuit between the sensing device and the computer. The digital measurements are recorded periodically by the computer as specified by the computer program. A thermometer reading may be recorded 100 times per second while the movement sensing photocell connected to the same process might be checked and recorded

500 times per second. A key feature of these computers is an internal clock that measures time in very small increments, such as thousandths of a second (milliseconds).

Process monitoring and control system output devices include devices such as solenoids and motor starters connected to the computer through a converter--in this case digital to analog. Basically, the converter changes a digital signal from the computer into an electric current that activates a physical device.

Process monitoring and control systems can also receive and send digital information. Typically, such systems include output display units that constantly show the state of the connected process or operation, and often they include logging devices that print the information for later analysis or reference.

b. Processing

Computers are often used for controlling a process or set of processes. Such computers are often called controllers, and the persons who work around them may not know even they are computers. This dedicated approach allows the design engineer to easily and safely match the computer speed with the requirements of the process.

Process control computers are also designed to provide clear warnings and calls for assistance when they fail. This is accomplished by warning devices such as horns, bells, warning lights, etc., that are automatically activated when the computer shuts down. These computers are also sometimes programmed to automatically shut down the processes or operations they control so as to prevent equipment or product damage or human injury.

c. Applications

Process monitoring and control systems have an almost endless variety of uses. Such systems might be found at work in a modern industrial plant performing such tasks as:

- Access control--controlling access to the premises through badge-reading devices and gate activators.
- Environment control--turning space heaters on or off as required and controlling the heat circulation system.
- Material handling--operating high-rise stacker cranes in warehouses to store and retrieve containers of materials.
- Machine tending--running machines through their cycles and activating the devices that feed raw material into and extract finished goods from them.

- Quality control--constantly measuring the quality of goods being produced, rejecting the bad items, and shutting down malfunctioning processes.

In the industrial plant examples given above, several computers of the same or different design and make might be used. Each use requires a different set of I/O devices, a different computer program, and all or part of the capacity of a computer.

Increasingly small but powerful process monitoring and control computers called microcomputers are being used in the office and home. Telephone switchboards and automatic typewriters are two common office uses of microcomputers. In the home, they are more often found in electric appliances, washing machines, television sets, and soon they will be used in automobiles. These uses require the high-volume production of identical and very small computer processors called microprocessors. The design and programming of the microprocessor is done during the design of the machine it will eventually become a part of. The programs are loaded into these computers during their manufacture and cannot be changed thereafter except by substituting a component.

d. Multiprogramming and Multiprocessing

Computer processors are much faster than the I/O devices connected to them. In a typical system the speed differences might be:

Device	Handling Capacity (characters per sec.)
Processor	3,000,000-10,000,000
Disk drive	600,000-3,000,000
Tape drive	100,000-2,000,000
Printer	500-1,500
Card reader	300-1,300
Terminal	30-600
Person	10-50

Early computer processors were usually idle and required to wait until the next piece of necessary information had been passed to it by one of the input devices and/or the finished information output had been received by an output device. Multiprogramming systems were developed to make fuller use of the computer processors by performing other operations asynchronously during the input/output wait times.

Operating Systems -- Operating systems consist of the programs that manage the computer operation and the connected I/O devices. Operating systems perform such functions as to transfer of data between the processor's storage and the devices, allocate storage space, determine which task will be performed next, keep a record of events, communicate with the computer operators, and often contain the system's compilers and various programs for general use as well. Operating systems are often large and complicated, consisting of up to millions of interrelated computer instructions.

The computer operator and/or user communicates with the computer through the operating system. He uses a special language often called "job control language," (JCL). Each operating system has its own control language designed to allow the user to direct the operation of the computer. These JCL statements are entered into the computer, usually by punching them onto cards that are then fed into a card reader. The operating system usually loads these JCL records into a storage unit where they wait their turn for processing in what is called a job queue.

Often the JCL statements are loaded onto a disk file when the job is originally created. This file of job control statements is known as the procedure library. Each set of job control statements in the procedure library is given a unique name or number identifier. The user then need enter only a single card containing the identifier to cause the operating system to retrieve and execute an entire set of job control statements from the procedure library.

The great majority of computer installations use operating systems supplied by the computer manufacturer, often with added operating system options purchased from other vendors. The basic operating system must be used because it is necessary to run the computer; but as in an automobile purchase, the buyer decides what options to use. Larger computer installations employ specialists known as systems programmers who work with the operating system. They analyze the options and recommend operating system options as needed, maintain the operating system, apply changes received from the operating system vendor, and evaluate and monitor the operating system performance.

Multiprogramming -- Multiprogramming systems permit more than one program to be executed simultaneously in the computer. When the program being processed is forced to pause to exchange data with an I/O device, the processor is switched by the operating system to execute another program until that program also is forced to pause, and so on.

Multiprogramming systems operate under the control of the computer operating system that performs many functions, including determining which of the several programs will be processed next. In some schemes, the programs are executed in rotation, and in others they are executed in prioritied order. In priority processing schemes, the jobs are given a relative priority rank when they are entered, and the operating system

always attempts to do the highest priority job next. If several programs of the same priority rank are waiting, the operating system will choose the one that has been waiting the longest time and will fit in available storage.

When a program has completed its tasks in a multiprogramming system, the operating system releases the space that program has been occupying in the computer and begins the task of reading in the next program. This program input task then becomes one of the processor's tasks. To ensure an uninterrupted flow of work to the processor, programs are loaded into the computer as soon as possible. The operating system stores these programs in a reserve area, usually a disk drive, until the necessary processor space and I/O devices are available. Other programs must wait until other requirements are met. Often a single computer job will contain several programs that must be run in a prescribed order. The operating system can initiate the first program in the job, but it must hold the second and subsequent programs in reserve until the first is complete, and so on.

Multiprocessing -- Multiprocessing consists of two or more connected processors under the control of a single operating system. This approach provides large computing capabilities. Multiprocessing advantages include the following:

- The interconnected processors can communicate directly with each other.
- Main storage and I/O devices can be shared by the processors and used more fully than if one set is dedicated to one processor and another set to another.
- Only one processor is required to run the operating system.
- Some degree of backup is available for processor failure.

D. DATA COMMUNICATIONS AND TELEPROCESSING

1. Communications Concepts

Data communications is defined as the transmission of digitized and computer processable information via communications circuits from one location to another. Teleprocessing is a form of a data processing that uses data communications.

Data communications and teleprocessing are used when it is necessary or more economical to physically separate the processing computer from the source of the input data, site of the output usage, or the computer user. Airline reservation systems are a common example. Reservation systems use data communications equipment and techniques to connect travel agents and airline personnel to a single computer or set of computers that is continually recording reservations, answering space availability inquiries, and performing other necessary central tasks.

High-capacity cables, capable of carrying hundreds of thousands of characters of information a second, connect computers to high-speed machines, such as other computers, disk drives, and tape drives. However, many machines connected to computers operate at much slower speeds. These slower machines are connected to the computer by lower capacity and less expensive cables that are similar to telephone or teletype lines. Direct cable connection becomes uneconomic at distances of more than 1 mile and usually before 2000 feet. When users miles away are communicating directly with a computer, they are said to be connected via a data communication circuit.

Two types of data communications circuits are analog circuits and digital circuits. The voice telephone network uses analog circuits capable of transmitting the full range of sounds that the human voice is capable of making. In a similar manner, the hands on a clock face can portray the full range of times in a 12-hour period. Analog communication is constantly and infinitely variable within a predetermined range.

Digital communiction circuits use the binary on-off principle to communicate information in digital form just as digital displays are now being used to express the time on digital clocks. Sounds can be converted by a computer into a series of digits that portray the volume, pitch, and other distinguishing characteristics. These digits can then be reconverted into sound by another computer at the receiving end. Digital circuits are capable of moving more information over a given distance in a given time than analog circuits and eliminate the noise distortion problems common to sound-carrying circuits. For these reasons, digital circuits are beginning to replace analog circuits in the telephone system, but this will be a gradual process over several years.

Data are transmitted at the speed of electricity, but one bit at a time. Typically 8 bits are needed to form one transmitted character. A normally functioning voice circuit is able to transmit 9600 bits per second, about 1200 characters per second. For comparison, people read at 50 bits or 6 characters per second and type at 15 bits or 2 characters per second. Slower transmission speeds are often used where possible so that slower or less expensive equipment can be used at each end of the circuit. It is also possible to go much faster than 1200 characters per second on certain types of special circuits available from communications carriers.

Transmission errors occur frequently, usually when the communication circuit is momentarily disrupted. These disruptions destroy some of the bits being transmitted thereby causing a condition known as parity error (counts of the numbers of zeros and ones are not correct). These parity errors are detected by the receiving equipment that notifies the communications control program in the central computer that an error has occurred. This program takes the necessary corrective action, usually retrying the transmission until error-free data have been achieved.

Most data communications today and through the 1980s will continue to use analog circuits. Digitized information to be transmitted is first converted to analog signals by a special device known as a modem (MOdulator-DEModulator), then reconverted to digital information by another modem at the receiving end. The analog circuits are obtained from a common carrier, usually the local telephone company. Data communications circuits may be regular dialed voice telephone lines capable of exchanging data with any other telephone line and equipped with a modem for digital-analog conversion. Other data communication circuits are analog telephone lines leased from the telephone company for the sole use of the subscriber. These leased dedicated lines cannot access or be accessed by the dial-up network. These leased lines also require modems to perform the necessary digital-analog conversions.

The two basic methods for transmitting information are known as asynchronous and synchronous. Asynchronous uses a starting bit of information followed at regular timed intervals by the bits representing a character followed by another start bit and so on. This is the least expensive and most widely used transmission method for low-speed systems.

The synchronous method uses a process called "hand-shaking" during which the sending and receiving device establishes a common clocking rate and transmits thereafter at the intervals specified by the clocking rate and without the need for the starting bits. Synchronous equipment requires internal clocking and is more expensive, but synchronous transmission does not need the starting bits to separate characters and is faster.

2. Communications Carriers

Communications carriers are the companies that supply facilities for transmitting analog and digital information. Several federally regulated companies provide most data communications services in the United States, using the existing voice facilities.

Other communications carriers often specialize in data communications and compete with or supplement the telephone company networks. Western Union, RCA, and ITT are among the better-known competitors licensed to operate as communications carriers within the United States. RCA, ITT, and Comsat Corporation also supply international communications services that carry data.

Carriers use a variety of technologies including high-data rate microwave facilities, satellites, and radio systems. Most carriers use several or all of these technologies, and a single signal may travel over land line, microwave, radio, and land line again before it completes its journey.

Recently another class of common carriers has begun offering what are known as "value-added networks". The value-added carriers such as

Tymnet use common carrier facilities and specialized data communications equipment to provide their service. These carriers develop a network using common carrier circuits connected through a computer or computers that add the capability to receive data from one source and send it to the addressee indicated in the content of the data received. This technique is known as "message-switching".

3. Teleprocessing

As noted earlier, data communications is used to connect a computer user to a physically distant computer. That user types at 15 bits per second and reads at 50 bits per second. He is connected to the computer via a data communications circuit that typically operates at speeds of 2400 to 9600 bits per second. The computer itself operates at speeds of 100 million bits per second. Evidently one user can use only a small portion of the communications circuit capacity and only a tiny fraction of the computer's capacity. Data communications systems are designed to use the excess computer and circuit capacity in several ways to reduce the overall cost.

Communication link costs are minimized by a design known as "multidropping". Many users at one place or in a geographic region are connected to a single communication line. As in a party line phone system each user's machine has a unique name or address. The computer calls each in turn to see if it is ready to receive or transmit data. This technique is know as "polling" and data communications lines designed in this manner are known as "multidrop".

Computer costs are minimized by allowing many users to share the same computer. A typical small computer can simultaneously operate several data communications lines at one time and larger computers can simultaneously work with dozens. The amount of work the computer must do to satisfy its users and the computers processing speed determine the capacity limit of these types of systems.

Another widely used technique known as "buffering" is designed to minimize both computer and communications line costs. Buffered designs require the user to use more expensive machines often containing small computers and that are able to store a small amount of data, usually 500 to 2000 characters. These buffered machines receive and send a group of characters in one continuous burst from the beginning to end of the data and up to the limits of the buffer size. These designs reduce the data communications management work of the computer and usually achieve higher data communications speeds. Users of these systems often experience a several-second delay before their information is sent to or received from the computer, usually because the communications line is busy with another buffered machine. Airlines reservation clerks and bank tellers both use machines of this type to work with the computers in their organizations.

These user-direct-to-computer systems operate under the control of a special computer program known as a "teleprocessing monitor". This program controls the transfer of information between the communication lines and the computer's storage and often does the user polling (turn-taking among users) as well. In other cases, specialized computers known as "front-end processors" are used to control the data communications, especially polling, and to notify the main computer when an information exchange is needed. Front-end processors are used to reduce the work load on the main computer, thereby enabling it to serve more lines and users.

Users may also be connected indirectly to a central computer, either through another computer located miles away or through other higher speed machines, such as computer tape drives or high-speed printers and card readers. These computer-to-computer and computer-to-higher speed machines are not bound by the speed of a user or users at their individual slower speed machines. Instead, whole processing jobs are performed without user intervention or interaction. These types of systems are known as "distributed processing" or "remote job entry". Typically these systems operate at much higher speeds and consume an entire communication line when operating. Therefore, lines are leased and dedicated for each remote job entry site.

The central computer also plays a key role in communication with the users who are indirectly connected. The communication occurs under the control of a special program in the central computer which is known as a "spooler". The records received from the users' machine must be immediately stored within the central computer in what is known as an "input queue". Similarly, output from the central computer to the users' machine must be put in anotner storage area known as the "output queue". This allows the users' machine to be a relatively simple and inexpensive device capable of performing only one function at a time. The user can schedule the work to and from the queues when he is ready and need not wait for the central computer unless he has caught up and the queues are empty.

a. Terminals

Terminals are machines that are able to send and/or receive digital information over a communication circuit. They may be attached directly to the computer by a local circuit or may be attached by a long-distance circuit many miles long. Terminals are the users means to send information to and receive information from a computer or another terminal, whether nearby or far away. Terminals may or may not have the ability to store information, and some do and some do not include a small computer for handling some functions independent of the control computer.

Many terminals are offered by a large number of suppliers. There are five major kinds of terminals with different capabilities:

- Typewriter-like terminals much like teletypes. These include a keyboard for entry of information and a printing device. These terminals supply a printed copy of what the computer sends back and usually of what the terminal operator has entered as well, but are slower and slightly more expensive than display terminals.

- Display terminals, sometimes known as cathode ray tubes or CRTs. These include a keyboard for entry of information and a screen like a television set for displaying information. These terminals are fast and easy to use, but are not able to supply a printed record of the information. If a printed record is necessary, a printing terminal must be added to the system. Display terminals are inexpensive and widely used.

- Intelligent terminals using a small computer. These terminals may have a wide variety of means for entering and receiving information; they are able to do local processing and to store and retrieve information. These are the most versatile terminals but are also more expensive.

- Remote batch terminals, usually a card reader and a high-speed line printer. These are used when high volumes of I/O must be handled; e.g., nearly always in a batch operation, such as a weekly payroll, etc.

- Specialized terminals, including a wide variety of specially designed devices for entering and receiving information. Examples include cash-dispensing machines, timekeeping terminals that are able to read and verify an employee's identification badge, special printers that prepare airline ticket stubs, etc. Specialized terminals are more expensive to engineer than standard terminals and are usually found in large organizations with an unusual combination of terminal requirements and a need for many such terminals that can absorb the engineering costs. Examples include airlines, large banks, and large facilities with stringent security requirements.

b. Computer Networks

The preceding discussions of data communications assumed one computer installation connected to local and remote users. However, there is also a need to interchange information among different computers and physically separated computers. The resulting complex of multiple computers equipped to move information from place to place by a communication network is known as a "computer network".

Computer networks are rapidly gaining acceptance as a faster, more economical method for moving information from one organization to another. Prominent examples include the banking industry that routinely

transfers trillions of dollars by means of computer-to-computer transactions via a network known as the electronic funds transfer system (EFTS). EFTS is now being spread to the international scene through a project called SWIFT that is cooperatively funded and operated by financial institutions in many nations.

Appendix A

FEDERAL COMPUTER-RELATED CRIME LEGISLATION

96th CONGRESS
1st SESSION

S. 240

(NOTE.—Fill in all blank lines except those provided for the date, number, and reference of bill.)

IN THE SENATE OF THE UNITED STATES

Mr. RIBICOFF (for himself) and Percy, Kennedy, Inouye, Jackson, Matsunaga, Moynihan, Williams, Zorinsky, Domenici, and Stevens

introduced the following bill; which was read twice and referred to the Committee on .....

A BILL

To amend title 18, United States Code, to make a crime the use, for fraudulent or other illegal purposes, of any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce.

(Insert title of bill here)

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled, That this Act may be cited as the "Federal Computer Systems Protection Act of 1979".

Sec. 2. The Congress finds that--

(1) computer related crime is a growing problem in the Government and in the private sector;

(2) such crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime;

(3) the copportunities for computer related crimes in Federal programs, in financial institutions, and in other entities which operate in interstate commerce through the introduction of fraudulent records into a computer system, unauthorized use of computer facilities, alteration or destruction of computerized information files, and stealing of financial instruments, data, or other assets, are great:

(4) computer related crime directed at institutions operating in interstate commerce has a direct effect on interstate commerce; and

(5) the prosecution of persons engaged in computer related crime is difficult under current Federal criminal statutes.

Sec. 3(a) Chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following new section:

"§1028. Computer fraud and abuse

"(a) Whoever knowingly and willfully, directly or indirectly accesses, causes to be accessed or attempts to access any computer, computer system, computer network, or any part thereof which, in whole or in part, operates in interstate commerce or is owned by, under contract to, or in conjunction with, any financial institution, the United States Government or any branch, department or agency thereof, or any entity operating in or affecting interstate commerce, for the purpose of:

(1) devising or executing any scheme or artifice to defraud, or

(2) obtaining money, property, or services, for themselves or another, by means of false or fraudulent pretenses, representations or promises, shall be fined a sum not more than two and one-half times the amount of the fraud or theft or imprisoned not more than 15 years or both.

"(b) Whoever intentionally and without authorization, directly or indirectly accesses, alters, damages, destroys, or attempts to damage or destroy any computer, computer system, or computer network described in subsection (a), or any computer software, program or data contained in such computer, computer system or computer network, shall be fined not more than $50,000 or imprisoned not more than 15 years, or both.

"(c) For purposes of this section, the term--

"(1) 'access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network;

"(2) 'computer" means an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network;

"(3) 'computer system' means a set of related, connected or unconnected, computer equipment, devices and software;

"(4) 'computer network' means the interconnection of communication systems with a computer through remote terminals, or a complex consisting of two or more interconnected computers;

"(5) 'property' includes, but is not limited to, financial instruments, information, including electronically processed or produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value;

"(6) 'services' includes, but is not limited to, computer time, data processing, and storage functions;

"(7) 'financial instrument' means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security, or any electronic data processing representation thereof;

"(8) 'computer program' means an instruction or statement or a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system;

"(9) 'computer software' means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system;

"(10) 'financial institution' means--

"(A) a bank with deposits insured by the Federal Deposit Insurance Corporation;

"(B) a member of the Federal Reserve including any Federal Reserve Bank;

"(C) an institution with accounts insured by the Federal Savings and Loan Insurance Corporation;

"(D) a credit union with accounts insured by the National Credit Union Administration;

"(E) a member of the Federal Home Loan Bank Systems and any Home Loan Bank;

"(F) a member or business insured by the Securities Investor Protection Corporation; and

"(G) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities and Exchange Act of 1934.".

(c) The table of sections of chapter 47 of title 18, United States Code, is amended by adding at the end thereof the following:

"1028. . . . . Computer fraud and abuse."

Appendix B

STATE COMPUTER-RELATED CRIME LAWS

television community antenna line service derived from any tampering, altering, or injury of any connection, wire, connector, device, altered meter, pipe, conduit, line, cable, transformer, amplifier, or other apparatus or device shall be prima facie evidence of intent to violate, and of the violation of, this section by the person or persons so using or receiving such direct benefits.

(4) Any person who willfully violates this section shall be guilty of a misdemeanor of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(5) Whoever is found in a civil action to have violated the provisions hereof shall be liable to the utility involved in an amount equal to three times the amount of services unlawfully obtained or $1,000, whichever is greater.

(6) Nothing in this act shall be construed to apply to licensed and certified electrical contractors while performing usual and ordinary service in accordance with recognized standards.

Laws 1976, c. 76-64, § 1, eff. Oct. 1, 1976. Amended by Laws 1978, c. 78-262, § 1, eff. July 1, 1978.

Laws 1978, c. 78-262, added subsec. (2)(c).

Library References
Electricity ⇨21.
Telecommunications ⇨449.
C.J.S. Electricity §§ 76, 77.
C.J.S. Telegraphs, Telephones, Radio and Television §§ 316.1, 316.2.

1. Validity
Presumption contained in this section that one in possession of real property where there is found to be existing connection, wire, conductor, meter alteration, or any device which affects the diversion of service of a utility is guilty of trespass and larceny with relation to utility fixtures is unconstitutional. MacMillan v. State, 358 So.2d 547 (1978).

CHAPTER 815. COMPUTER-RELATED CRIMES [NEW]

See.
815.01 Short title.
815.02 Legislative intent.
815.03 Definitions.
815.04 Offenses against intellectual property.
815.05 Offenses against computer equipment or supplies.
815.06 Offenses against computer users.
815.07 This chapter not exclusive.

815.01 Short title

The provisions of this act shall be known and may be cited as the "Florida Computer Crimes Act."

Added by Laws 1978, c. 78-92, § 2, eff. Aug. 1, 1978.

Library References
Trade Regulations ⇨861.
C.J.S. Trade-Marks, Trade-Names and Unfair Competition § 237.

815.02 Legislative intent

The Legislature finds and declares that:

(1) Computer-related crime is a growing problem in government as well as in the private sector.

(2) Computer-related crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime.

(3) The opportunities for computer-related crimes in financial institutions, government programs, government records, and other business enterprises through the introduction of fraudulent records into a computer system, the unauthorized use of computer facilities, the alteration or destruction of computerized information or files, and the stealing of financial instruments, data, and other assets are great.

(4) While various forms of computer crime might possibly be the subject of criminal charges based on other provisions of law, it is appropriate and desirable that a supplemental and additional statute be provided which proscribes various forms of computer abuse.

Added by Laws 1978, c. 78-92, § 1, eff. Aug. 1, 1978.

815.03 Definitions

As used in this chapter, unless the context clearly indicates otherwise:

(1) "Intellectual property" means data, including programs.

(2) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data.

(3) "Computer" means an internally programmed, automatic device that performs data processing.

(4) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(5) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, or computer software.

(6) "Computer network" means a set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities.

(7) "Computer system services" means providing a computer system or computer network to perform useful work.

(8) "Property" means anything of value as defined in s. 812.011 and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine-readable or human-readable form, and any other tangible or intangible item of value.

(9) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.

(10) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

Added by Laws 1978, c. 78-92, § 1, eff. Aug. 1, 1978.

Library References
Words and Phrases (Perm.Ed.)

815.04 Offenses against intellectual property

(1) Whoever willfully, knowingly, and without authorization modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(2) Whoever willfully, knowingly, and without authorization destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(3) Whoever willfully, knowingly, and without authorization discloses or takes data, programs, or supporting documentation which is a trade secret as defined in s. 812.081 or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network commits an offense against intellectual property.

(4)(a) Except as otherwise provided in this subsection, an offense against intellectual property is a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(b) If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

Added by Laws 1978, c. 78-92, § 1, eff. Aug. 1, 1978.

815.05 Offenses against computer equipment or supplies

(1) Whoever willfully, knowingly, and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network commits an offense against computer equipment or supplies.

(b) 1. Except as provided in this paragraph, an offense against computer equipment or supplies as provided in paragraph (a) is a misdemeanor of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

2. If the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, then the of-

fender is guilty of a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(2)(a) Whoever willfully, knowingly, and without authorization destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization destroys, injures, or damages any computer, computer system, or computer network commits an offense against computer equipment or supplies.

(b) 1. Except as provided in this paragraph, an offense against computer equipment or supplies as provided in paragraph (a) is a misdemeanor of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

2. If the damage to such computer equipment or supplies or to the computer, computer system, or computer network is greater than $200 but less than $1,000, then the offender is guilty of a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

3. If the damage to such computer equipment or supplies or to the computer, computer system, or computer network is $1,000 or greater, or if there is an interruption or impairment of governmental operation or public communication, transportation, or supply of water, gas, or other public service, then the offender is guilty of a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

Added by Laws 1978, c. 78-92, § 1, eff. Aug. 1, 1978.

815.06 Offenses against computer users

(1) Whoever willfully, knowingly, and without authorization accesses or causes to be accessed any computer, computer system, or computer network; or whoever willfully, knowingly, and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with another commits an offense against computer users.

(2)(a) Except as provided in this subsection, an offense against computer users is a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

(b) If the offense is committed for the purposes of devising or executing any scheme or artifice to defraud or to obtain any property, then the offender is guilty of a felony of the second degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

Added by Laws 1978, c. 78-92, § 1, eff. Aug. 1, 1978.

815.07 This chapter not exclusive

The provisions of this chapter shall not be construed to preclude the applicability of any other provision of the criminal law of this state which presently applies or may in the future apply to any transaction which violates this chapter, unless such provision is inconsistent with the terms of this chapter.

Added by Laws 1978, c. 78-92, § 1, eff. Aug. 1, 1978.

CHAPTER 817. FRAUDULENT PRACTICES

817.035 Schemes to defraud; proof; penalties

(1) Any person who engages in a scheme constituting a systematic, ongoing course of conduct with intent to defraud more than one person, or to obtain property from more than one person by false or fraudulent pretenses, representations, or promises, and who so obtains property from one or more of such persons is guilty of a misdemeanor of the first degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

ARTICLE 5.5

Computer Crime

18-5.5-101. Definitions. As used in this article, unless the context otherwise requires:

(1) To "use" means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.

(2) "Computer" means an electronic device which performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network.

(3) "Computer network" means the interconnection of communication lines (including microwave or other means of electronic communication) with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

(H)

(4) "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system.

(5) "Computer software" means computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(6) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, and software.

(7) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, debit card, or marketable security.

(8) "Property" includes, but is not limited to financial instruments, information, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

(9) "Services" includes, but is not limited to, computer time, data processing, and storage functions.

18-5.5-102. Computer crime. (1) Any person who knowingly uses any computer, computer system, computer network, or any part thereof for the purpose of: devising or executing any scheme or artifice to defraud, obtaining money, property, or services by means of false or fraudulent pretences, representations, or promises, or committing theft, commits computer crime.

(2) Any person who knowingly and without authorization

uses, alters, damages, or destroys any computer, computer system, or computer network described in section 18-5.5-101 or any computer software, program, documentation, or data contained in such computer, computer system, or computer network commits computer crime.

(3) If the loss, damage, or thing of value taken in violation of this section is less than fifty dollars, computer crime is a class 3 misdemeanor; if fifty dollars or more but less than two hundred dollars, computer crime is a class 2 misdemeanor; if two hundred dollars or more but less than ten thousand dollars, computer crime is a class 4 felony; if ten thousand dollars or more, computer crime is a class 3 felony.

SECTION 8. 18-6-401 (7), Colorado Revised Statutes 1973, 1978 Repl. Vol., is amended to read:

18-6-401. Child abuse. (7) Child abuse is a class 2 misdemeanor, but if it results in serious bodily injury to the child OR DEATH OF THE CHILD, it is a class 3 felony.

SECTION 9. Part 1 of article 8 of title 18, Colorado Revised Statutes 1973, 1978 Repl. Vol., is amended BY THE ADDITION OF A NEW SECTION to read:

18-8-115. Duty to report a crime. It is the duty of every corporation or person who has reasonable grounds to believe that a crime has been committed to report promptly the suspected crime to law enforcement authorities. When acting in good faith, such corporation or person shall be immune from any civil liability for such reporting. This duty shall exist

(p) False statements or publications concerning land for sale or lease or sale of subdivided lands or sale and mortgaging of unsubdivided lands.

(q) Resale of realty with intent to defraud.

(r) Fraud in purchase or sale of securities.

(s) Sale of unregistered securities or real property securities and transactions involving such securities by unregistered dealers or salesmen.

(t) A scheme or artifice to defraud.

5. "Records" means any book, paper, writing, record, computer program or other material.

E. For the purposes of § 13-2316:

1. "Access" means to approach, instruct, communicate with, store data in, retrieve data from or otherwise make use of any resources of a computer, computer system or computer network.

2. "Computer" means an electronic device which performs logic, arithmetic or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, software or communication facilities which are connected or related to such a device in a system or network.

3. "Computer network" means the interconnection of communication lines with a computer through remote terminals or a complex consisting of two or more interconnected computers.

4. "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system.

5. "Computer software" means a set of computer programs, procedures and associated documentation concerned with the operation of a computer system.

6. "Computer system" means a set of related, connected or unconnected computer equipment, devices and software.

7. "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, marketable security or any other written instrument, as defined by § 13-2001, paragraph 7, which is transferable for value.

8. "Property" means financial instruments, information, including electronically produced data, computer software and programs in either machine or human readable form, and anything of value, tangible or intangible.

9. "Services" includes computer time, data processing and storage functions.

Added Laws 1977, Ch. 142, § 82, eff. Oct. 1, 1978. As amended Laws 1978, Ch. 201, § 151, eff. Oct. 1, 1978; Laws 1978, Ch. 204, § 1, eff. Oct. 1, 1978.

Historical Note

Source:

Pen.Code 1901, §§ 469–472.
Pen.Code 1913, §§ 512–515.
Rev.Code 1928, §§ 4770, 4771.
Code 1939, §§ 43–1901; 43–1902.
A.R.S. former § 13–401.

Subsec. A, pars. 1 to 7, were adopted from the United States Code; see 18 U.S.C.A. §§ 891 through 894.

Laws 1978, Ch. 201, § 151, substituted "§ 13-2308" for "§ 13-2313" in the introductory phase of subsec. C., substituted "or enterprises" for "corporations or partnerships", and "conduct which violates" for "violation of", deleted "of this title or of the criminal or penal provisions" following "or more provisions", "or ordinance" following "felony statute", and "in" following "of this state", and inserted "felony" following "provisions of any" in the first sentence of paragraph 2 of subsec. C.; and deleted subds. (a) through (i) of paragraph 2 of subsec. C. which had read:

"(a) Trafficking in narcotic drugs or dangerous drugs, explosives, alcoholic beverages, weapons, tobacco or stolen property.
"(b) Gambling.
"(c) Prostitution.
"(d) Extortion.
"(e) Coercion.
"(f) Usury.
"(g) Forgery.
"(h) Theft.
"(i) Asserting false claims including, but not limited to, false claims asserted through fraud or arson."

Laws 1978, Ch. 204, § 1, substituted "13-2308" for "13-2313" in the introductory phrase of subsec. C., and added subsecs. D. and E.

Laws 1978, Ch. 204, § 4 provides:
"The provisions of this act shall become effective on October 1, 1978."

1978 Reviser's Note:

This section contains the amendments made by Laws 1978, chapter 201, section 151 and chapter 204, section 1 which were blended together as shown above pursuant to authority of section 41-1304.03.

Cross References

Judicial powers over racketeering criminal cases, see § 13-2313.
Racketeering,
Civil remedies, see § 13-2314.
Racketeering,
Investigation of records, see § 13-2315.

§ 13-2302. Making extortionate extensions of credit; classification

A. Any person who makes an extortionate extension of credit is guilty of a class 5 felony.

B. In any prosecution pursuant to this section, if it is shown that all of the following factors were present in connection with the extension of credit, there is prima facie evidence that the extension of credit was extortionate:

criminal liability against such custodian or financial institution in any action brought alleging violation of the confidentiality of such records.

B. The attorney general or the authorized county attorney may petition the superior court for enforcement of this section in the event of noncompliance with the request for inspection. Enforcement shall be granted if the request is reasonable and the attorney general or the authorized county attorney has reasonable grounds to believe the records sought to be inspected are relevant to a civil or criminal investigation of an offense included in the definition of racketeering in § 13-2301, subsection D, paragraph 4 or a violation of § 13-2312.

C. The investigation authority granted pursuant to the provisions of this section may not be exercised by a county attorney in the absence of authorization by the attorney general.

D. Any person releasing information obtained pursuant to this section, except in the proper discharge of official duties, is guilty of a class 2 misdemeanor.

Added Laws 1978, Ch. 204, § 2, eff. Oct. 1, 1978.

Adopted from the United States Code; see 18 U.S.C.A. §§ 1961 through 1968.

"classification" was substituted for "penalty".

1978 Reviser's Note:

Pursuant to authority of section 41-1304.02, in the heading of this section

§ 13-2316. Computer fraud; classification

A. A person commits computer fraud in the first degree by accessing, altering, damaging or destroying without authorization any computer, computer system, computer network, or any part of such computer, system or network, with the intent to devise or execute any scheme or artifice to defraud or deceive, or control property or services by means of false or fraudulent pretenses, representations or promises.

B. A person commits computer fraud in the second degree by intentionally and without authorization accessing, altering, damaging or destroying any computer, computer system or computer network or any computer software, program or data contained in such computer, computer system or computer network.

C. Computer fraud in the first degree is a class 3 felony. Computer fraud in the second degree is a class 6 felony.

Added Laws 1978, Ch. 204, § 2, eff. Oct. 1, 1978.

Historical Note

For effective date provision of Laws 1978, Ch. 204, see note following § 13-2301.

Cross References

Computer fraud, definition of terms, see § 13-2301.

(As Amended)

79—H 5775

Introduced by—
Representative DeAngelis

Ordered Printed by—
House of Representatives

Referred to—
House Committee on Judiciary

Date Printed—
March 27, 1979

State of Rhode Island and Providence Plantations

JANUARY SESSION, A.D. 1979

AN ACT Relating to Criminal Law.

It is enacted by the General Assembly as follows:

Section 1. Title 11 of the general laws entitled "Criminal Offenses" is hereby amended by adding the following chapter:

"CHAPTER 51
"COMPUTER CRIME

"11-51-1. DEFINITIONS. — As used in this chapter: (A) 'Access' means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network.

(B) 'Computer' means an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage,

software, or communication facilities which are connected or related to such a device in a system or network.

(C) 'Computer system' means a set of related, connected or unconnected, computer equipment, devices and software.

(D) 'Computer network' means the interconnection of communication lines with a computer through remote terminals, or a complex consisting of two or more interconnected computers.

(E) 'Property' includes, but is not limited to, financial instruments, information, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

(F) 'Services' includes, but is not limited to, computer time, data processing, and storage functions.

(G) 'Computer program' means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer systems.

(H) 'Computer software' means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

"11-51-2. ACCESS TO COMPUTER FOR FRAUDULENT PURPOSES. — Whoever directly or indirectly accesses or causes to be accessed any computer, computer system, or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or (2) obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises shall be guilty of a felony and shall be subject to the penalties set forth in section 11-51-4.

"11-51-3. INTENTIONAL ACCESS, ALTERATION, DAMAGE OR DESTRUCTION. — Whoever intention-

CONTINUED

3 OF 5

ally and without authorization, directly or indirectly accesses, alters, damages, or destroys any computer, computer system, computer network, computer software, computer program or data contained in such computer, computer system, computer program or computer network shall be guilty of a felony and shall be subject to the penalties set forth in section 11-51-4.

"11-51-4. PENALTIES. — Any person who is convicted of the offenses set forth in sections 11-51-2 and 11-51-3 shall be fined not more than five thousand dollars ($5,000) or imprisoned for not more than five (5) years, or both.

Sec. 2. This act shall take effect upon passage.

79-H 5775

EXPLANATION

By the Legislative Council

This act would make certain acts relating to computers and computer systems criminal offenses and provide for penalties for commission of the offenses.

This act would take effect upon passage.

The Legislature

of the

State of New Mexico

34th Legislature, 1st Session

LAWS 1979

CHAPTER 176

SENATE JUDICIARY COMMITTEE SUBSTITUTE FOR SENATE BILL 8,

with certificate of correction

Introduced by

CHAPTER 176

AN ACT

RELATING TO COMPUTER USE; AMENDING THE CRIMINAL CODE TO MAKE MISUSE OF COMPUTERS A CRIME.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF NEW MEXICO:

Section 1. SHORT TITLE.--This act may be cited as the "Computer Crimes Act".

Section 2. DEFINITIONS.--As used in the Computer Crimes Act:

A. "access" means to make use of any resources of a computer, computer system or computer network;

B. "computer" means an electronic device which performs logical, arithmetic and memory functions by the manipulation of electronic or magnetic impulses and includes all input, output, processing, storage, software or communication facilities which are connected or related to such a device in a computer system or computer network;

C. "computer network" means the interconnection of communication lines with a computer through remote terminals or a complex consisting of two or more computers and includes interconnected remote terminals;

D. "computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from a computer system;

E. "computer software" means a set of computer programs,

procedures and associated documentation concerned with the operation and function of a computer system; and

F. "computer system" means a set of related or interconnected computer equipment, devices and software.

Section 3. COMPUTER FRAUD.--

A. Any person who accesses or causes to be accessed any computer, computer system, computer network or any part thereof with the intent to devise or execute any scheme or artifice to defraud is guilty of a fourth degree felony.

B. Any person who accesses or causes to be accessed any computer, computer system, computer network or any part thereof with the intent to obtain, by means of embezzlement or false or fraudulent pretenses, representations or promises, money, property or services where:

(1) the money, property or services have a value of one hundred dollars ($100) or less, is guilty of a petty misdemeanor;

(2) the money, property or services have a value of more than one hundred dollars ($100) but not more than two thousand five hundred dollars ($2,500), is guilty of a fourth degree felony; or

(3) the money, property or services have a value of more than two thousand five hundred dollars ($2,500), is guilty of a third degree felony.

Section 4. UNAUTHORIZED COMPUTER USE.--Any person who intentionally, maliciously and without authorization accesses, alters,

damages or destroys any computer, computer system, computer network, any part thereof or any information stored therein when:

A. the computer, computer system, computer network, part or information has a value of one hundred dollars ($100) or less is guilty of a petty misdemeanor;

B. the computer, computer system, computer network, part or information has a value of more than one hundred dollars ($100) but not more than two thousand five hundred dollars ($2,500) is guilty of a fourth degree felony; or

C. the computer, computer system, computer network, part or information has a value of more than two thousand five hundred dollars ($2,500) is guilty of a third degree felony.

STATE OF MICHIGAN
80TH LEGISLATURE
REGULAR SESSION OF 1979

Introduced by Reps. Bennane, Vaughn, Bullard, Mary C. Brown, Spaniola, Vanek, Watkins, Tomboulian, Busch and Cushingberry

ENROLLED HOUSE BILL No. 4112

AN ACT to prohibit access to computers, computer systems, and computer networks for certain fraudulent purposes; to prohibit intentional and unauthorized access, alteration, damage, and destruction of computers, computer systems, computer networks, computer software programs, and data; and to prescribe penalties.

The People of the State of Michigan enact:

Sec. 1. For the purposes of this act, the words and phrases defined in sections 2 and 3 have the meanings ascribed to them in those sections.

Sec. 2. (1) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise use the resources of, a computer, computer system, or computer network.

(2) "Computer" means an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses, and includes input, output, processing, storage, software, or communication facilities which are connected or related to a device in a system or network.

(3) "Computer network" means the interconnection of communication lines with a computer through remote terminals, or a complex consisting of 2 or more interconnected computers.

(4) "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from the computer system.

(5) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(6) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, and software.

Sec. 3. (1) "Property" includes financial instruments; information, including electronically produced data; computer software and programs in either machine or human readable form; and any other tangible or intangible item of value.

(2) "Services" includes computer time, data processing, and storage functions.

Sec. 4. A person shall not, for the purpose of devising or executing a scheme or artifice with intent to defraud or for the purpose of obtaining money, property, or a service by means of a false or fraudulent pretense, representation, or promise with intent to, gain access to or cause access to be made to a computer, computer system, or computer network.

Sec. 5. A person shall not intentionally and without authorization, gain access to, alter, damage, or destroy a computer, computer system, or computer network, or gain access to, alter, damage, or destroy a computer software program or data contained in a computer, computer system, or computer network

Sec. 6. A person shall not utilize a computer, computer system, or computer network to commit a violation of section 174 of Act No. 328 of the Public Acts of 1931, as amended, being section 750.174 of the Michigan Compiled Laws, section 279 of Act No. 328 of the Public Acts of 1931, being section 750.279 of the Michigan Compiled Laws, section 356 of Act No. 328 of the Public Acts of 1931, as amended, being section 750.356 of the Michigan Compiled Laws, or section 362 of Act No. 328 of the Public Acts of 1931, as amended, being section 750.362 of the Michigan Compiled Laws.

Sec. 7. A person who violates this act, if the violation involves $100.00 or less, is guilty of a misdemeanor. If the violation involves more than $100.00, the person is guilty of a felony, punishable by imprisonment for not more than 10 years, or a fine of not more than $5,000.00, or both.

Clerk of the House of Representatives.

Secretary of the Senate.

Approved.....

.....

Governor.

Appendix C

PROPOSED COMPUTER-RELATED CRIME LEGISLATION

CALIFORNIA

AMENDED IN ASSEMBLY AUGUST 28, 1979
AMENDED IN ASSEMBLY JULY 16, 1979
AMENDED IN ASSEMBLY JUNE 19, 1979
AMENDED IN SENATE MAY 17, 1979
AMENDED IN SENATE MAY 9, 1979
AMENDED IN SENATE APRIL 23, 1979
AMENDED IN SENATE FEBRUARY 15, 1979

SENATE BILL No. 66

Introduced by Senator Cusanovich

December 5, 1978

An act to add Section 502 to the Penal Code, relating to computer crime.

LEGISLATIVE COUNSEL'S DIGEST

SB 66, as amended, Cusanovich. Computer crime.

Existing law relative to crimes involving fraud, or unauthorized access to, or damage or destruction of, property does not contain any specific provision relative to computers.

This bill would make it a crime, as specified, to intentionally access or cause to be accessed any computer system, or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or extort or (2) obtaining money, property or services with false or fraudulent intent, representations, or promises, or to maliciously access, alter, delete, damage, or destroy any computer system, computer network, computer program, or data.

Under existing law, Sections 2231 and 2234 of the Revenue and Taxation Code require the state to reimburse local agencies and school districts for certain costs mandated by the state. Other provisions require the Department of Finance to

review statutes disclaiming these costs and provide, in certain cases, for making claims to the State Board of Control for reimbursement.

This bill provides that no appropriation is made by this act pursuant to Section 2231 and 2234 for a specified reason, but recognizes that local agencies and school districts may pursue their other available remedies to seek reimbursement for these costs.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program. yes.

The people of the State of California do enact as follows:

SECTION 1. Section 502 is added to the Penal Code, to read:

502. (a) For purposes of this section:

(1) "Access" means to instruct, communicate with, store data in, or retrieve data from a computer system or computer network.

(2) "Computer system" means a machine or collection of machines, excluding pocket calculators *which are not programmable and capable of being used in conjunction with external files*, one or more of which contain computer programs and data, that performs functions, including, but not limited to, logic, arithmetic, data storage and retrieval, communication, and control.

(3) "Computer network" means an interconnection of two or more computer systems.

(4) "Computer program" means an ordered set of instructions or statements, and related data that, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions.

(5) "Data" means a representation of information, knowledge, facts, concepts, or instructions, which are being prepared or have been prepared, in a formalized manner, and are intended for use in a computer system or computer network.

(6) "Financial instrument" includes, but is not limited to, any check, draft, warrant, money order, note,

certificate of deposit, letter of credit, bill of exchange, credit or debit card, transaction authorization mechanism, marketable security, or any computer system representation thereof.

(7) "Property" includes, but is not limited to, financial instruments, data, computer programs, documents associated with computer systems and computer programs, or copies thereof, whether tangible or intangible, including both human and computer system readable data, and data while in transit.

(8) "Services" includes, but is not limited to, the use of the computer system, computer network, computer programs, or data prepared for computer use, or data contained within a computer system, or data contained within a computer network.

(b) Any person who intentionally accesses or causes to be accessed any computer system or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or extort or (2) obtaining money, property, or services with false or fraudulent intent, representations, or promises shall be guilty of a public offense.

(c) Any person who maliciously accesses, alters, deletes, damages, or destroys any computer system, computer network, computer program, or data shall be guilty of a public offense.

(d) Any person who violates the provisions of subdivision (b) or (c) is guilty of a felony and is punishable by a fine not exceeding five thousand dollars ($5,000), or by imprisonment in the state prison for 16 months, or two or three years, or by both such fine and imprisonment, or by a fine not exceeding two thousand five hundred dollars ($2,500), or by imprisonment in the county jail not exceeding one year, or by both such fine and imprisonment.

(e) This section shall not be construed to preclude the applicability of any other provision of the criminal law of this state which applies or may apply to any transaction.

SEC. 2. Notwithstanding Section 2231 or 2234 of the Revenue and Taxation Code, no appropriation is made by

this act pursuant to these sections because this act creates a new crime or infraction, eliminates a crime or infraction, or changes the penalty for a crime or infraction. It is recognized, however, that a local agency or school district may pursue any remedies to obtain reimbursement available to it under Chapter 3 (commencing with Section 2201) of Part 4 of Division 1 of that code.

O

(To be made one and twelve copies)
THE SENATE
TENTH..... LEGISLATURE, 19 79.
STATE OF HAWAII

S.B. NO. 504

A BILL FOR AN ACT

RELATING TO COMPUTER CRIMES.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF HAWAII:

SECTION 1. The legislature finds that:

(1) Computer-related crime is a growing problem in the government and in the private sector;

(2) Such crime occurs at great cost to the public since losses for each incident of computer crime tend to be far greater than the losses associated with each incident of other white collar crime;

(3) The opportunities for computer-related crimes in government programs, in financial institutions, and in other entities through the introduction of fraudulent records into a computer system, unauthorized use of computer facilities, alteration or destruction of computerized information files, and stealing of financial instruments, data, or other assets, are great; and

(4) The prosecution of persons engaged in computer-related crime is difficult under current state criminal statutes.

SECTION 2. Chapter 708, Hawaii Revised Statutes, is amended by adding a new section to be appropriately designated and to read:

"Sec. 708- Computer fraud. (1) A person commits the offense of computer fraud if the person:

(a) Indirectly or directly, accesses or causes to be accessed any computer, computer system, computer network, or any part thereof for the purposes of:

(i) Devising or executing any scheme or artifice to defraud, or

(ii) Obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises.

(b) Intentionally and without authorization, directly or indirectly, accesses, alters, damages, or destroys any computer, computer system, or computer network, or any computer software, program, or data contained in such computer, computer system, or computer network.

(2) For purposes of this section:

(a) "Access" means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of: a computer, computer system, or computer network;

(b) "Computer" means an electronic device which performs logical, arithmetic, and memory functions by the manipulations of electronic or magnetic impulses, and includes all input, output, processing, storage, software, or communication facilities which are connected or related to such a device in a system or network;

(c) "Computer network" means the interconnection of communication lines with a computer through remote terminals, or a complex consisting of two or more interconnected computers;

(d) "Computer program" means a series of instructions or statements, in a form acceptable to a computer, which permits the functioning of a computer system in a manner designed to provide appropriate products from such computer system;

(e) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system;

S.B.NO. 504

(f) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, and software;

(g) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security;

(h) "Property" includes, but is not limited to, financial instruments, information, including electronically produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value; and

(i) "Services" includes, but is not limited to, computer time, data processing, and storage functions.

(3) Computer fraud is a class A felony."

SECTION 3. New statutory material is underscored.

SECTION 4. This Act shall take effect upon its approval.

INTRODUCED BY: Jack S. Carroll

2/6/79

HOUSE BILL 1027

HB1027

81st GENERAL ASSEMBLY
State of Illinois

1979 and 1980

INTRODUCED March 21, 1979, BY Representatives Waddell--Brady--White, Ryan, Madigan, Friedland, Matijevich, E. M. Barnes, Bianco, Birkinbine, Boucek, Bower, Davis, Epton, Flinn, D.P.Friedrich, Giorgi, Hallock, Hallstrom, Huskey, Dave Jones, Kane, Keane, Kelly, Kempiners, Kent, Klosak, Lechowicz, Macdonald, Mahar, Margalus, Matula, Mautino, McAuliffe, McCourt, Mulcahey, Murphy, Polk, Pullen, Redmond, Reilly, Rigney, Schisler, Schoeberlein, Sharp, Simms, Stanley, E. G. Steele, C. M. Stiehl, Telcser, Van Duyne, Vinson, Vitek, Walsh, Bullock and White.c

SYNOPSIS: (Ch. 38, pars. 15-1 and 15-7, new par. 16-9)

Amends the Criminal Code. Makes it a criminal offense to use a computer or alter or destroy computer programs without the consent of the owner of the system. Effective immediately.

LRB8104934KPjw

A BILL FOR

275

AN ACT to add Section 16-9 to and to amend Sections 15-1 and 15-7 of the "Criminal Code of 1961", approved July 28, 1961, as amended.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 1. Sections 15-1 and 15-7 of the "Criminal Code of 1961", approved July 28, 1961, as amended, are amended, and Section 16-9 is added thereto, the added and amended Sections to read as follows:

(Ch. 38, par. 15-1)

Sec. 15-1. Property. As used in this Part C, "property" means anything of value. Property includes real estate, money, commercial instruments, admission or transportation tickets, written instruments representing or embodying rights concerning anything of value, labor, or services, or otherwise of value to the owner; things growing on, affixed to, or found on land, or part of or affixed to any building; electricity, gas and water; birds, animals and fish, which ordinarily are kept in a state of confinement; food and drink; samples, cultures, microorganisms, specimens, records, recordings, documents, blueprints, drawings, maps, and whole or partial copies, descriptions, photographs, computer programs or data, prototypes or models thereof, or any other articles, materials, devices, substances and whole or partial copies, descriptions, photographs, prototypes, or models thereof which constitute, represent, evidence, reflect or record a secret scientific, technical, merchandising, production or management information, design, process, procedure, formula, invention, or improvement.

(Ch. 38, par. 15-7)

Sec. 15-7. Obtain. As used in this Part C, "obtain" means:

(a) In relation to property, to bring about a transfer

of interest, or possession or use, whether to the offender or to another, and

(b) In relation to labor or services, to secure the performance thereof.

(Ch. 38, new par. 16-9)

Sec. 16-9. Unlawful use of a computer. (a) As used in this Part C:

1. "Computer" means an internally programmed, general purpose digital device capable of automatically accepting data, processing data and supplying the results of the operation.

2. "Computer system" means a set of related, connected devices, including a computer and other devices, including but not limited to data input and output and storage devices, data communications links, and computer programs and data, that make the system capable of performing the special purpose data processing tasks for which it is specified.

3. "Computer program" means a series of coded instructions or statements in a form acceptable to a computer, which causes the computer to process data in order to achieve a certain result.

(b) A person commits unlawful use of a computer when he:

1. Obtains the use of a computer system, or any part thereof, without the consent of the owner; or

2. Alters or destroys computer programs or data without the consent of the owner of the computer system; or

3. Intentionally, knowingly or recklessly obtains use of, alters or destroys a computer system, or any part thereof, as part of a scheme to defraud, obtain money, property or services from the owner of a computer or any third party.

(c) Sentence:

1. A person convicted of a violation of subsections (b)(1) or (2) of this Section where the value of the use, alteration, or destruction is $150.00 or less shall be guilty

HB1027

of a petty offense.

2. A person convicted of a violation of subsections (b) (1) or (2) of this Section where the value of the use, alteration or destruction is more than $1,000 shall be guilty of a Class A misdemeanor.

3. A person convicted of a violation of subsection (b) (3) of this Section shall be guilty of a Class 4 felony.

(d) This Section shall neither enlarge nor diminish the rights of parties in civil litigation.

Section 2. This Act takes effect on becoming a law.

OFFERED IN COMMITTEE ON JUDICIARY II BY REP.

LRB8104939SJfbam01

AMENDMENT TO HOUSE BILL 1027

AMENDMENT NO. 1. Amend House Bill 1027 on page 1, lines 1 and 2 and line 6, by deleting "Sections 15-1 and 15-7" and inserting in lieu thereof "Section 15-1"; and

on page 1, line 7, by deleting "are" and inserting in lieu thereof "is"; and

by deleting the unnumbered line after line 28 and lines 29 through 31 on page 1 and lines 1 through 4 on page 2; and

on page 2, by deleting lines 22 through 30 and inserting in lieu thereof the following:

"1. Knowingly obtains the use of a computer system, or any part thereof, without the consent of the owner (as defined in Section 15-2); or

2. Knowingly alters or destroys computer programs or data without the consent of the owner (as defined in Section 15-2); or

3. Knowingly obtains use of, alters or destroys a computer system, or any part thereof, as part of a deception for the purpose of obtaining money, property or services from the owner of a computer system (as defined in Section 15-2) or any third party."; and

on page 3, by deleting line 7 and inserting in lieu thereof

the following:

"(3) of this Section where the value of the money, property or services obtained is $1,000 or less shall be guilty of a Class A misdemeanor.

4. A person convicted of a violation of subsection (b)(3) of this Section where the value of the money, property or services obtained is more than $1,000 shall be guilty of a Class 4 felony.".

79-2510 <REVISOR > RK

Introduced by Stumpf, Spear, McCutcheon, Moe, Kirchner
March 26th, 1979
Ref to Com. on Judiciary

S.F. No. 1033

Companion H.F. No. 1003
Ref. to H. Com. on 3/26 Criminal Justice

Reproduced by PHILLIPS LEGISLATIVE SERVICE, INC.

Authors: Kahn, Bailey, D. Anderson, McCarron, Pavlakis

Computer Crimes

S.F.No.1033-Committee on Judiciary
Introduced by Stumpf x(St. Paul) Spear x(Mpls) McCutcheon x(St. Paul) Moe x(Ada) Kirchner*(Richfield) New legislation making it a crime to carry on certain activities in connection with data processing equipment. Sets penalties for modifying or destroying data processing data, programs or supporting documentaion, disclosing or taking these when they are trade secrets or confidential and modifying computer equipment or supplies without authorization, when they involve fraud. Sets penalties for intentional destruction or damage, without authorization, of computer equipment or supplies. Further sets penalties for unauthorized access to computers and for denial of computer services to authorized users of computer systems when they involve fraud.

A bill for an act

relating to crimes; specifying offenses relating to computers; providing penalties.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. [609.8611 [DEFINITIONS.] Subdivision 1. For the purposes of sections 1 to 8, the terms defined in this section have the meanings given them.

Subd. 2. "Intellectual property" means data including programs.

Subd. 3. "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data.

Subd. 4. "Computer" means an internally-programmed, automatic device that performs data processing.

Subd. 5. "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

Subd. 6. "Computer system" means a set of related, connected or unconnected, computer equipment, devices, or

computer software.

Subd. 7. "Computer network" means a set of related, remotely connected devices and communication facilities including more than one computer system with capability to transmit data among them through communication facilities.

Subd. 8. "Computer system services" means providing a computer system or computer network to perform useful work.

Subd. 9. "Property" means anything of value and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

Subd. 10. "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.

Subd. 11. "Access" means to approach, instruct, communicate with, store data, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network.

Sec. 2. [609.862] [OFFENSE AGAINST INTELLECTUAL PROPERTY.] Whoever intentionally and without authorization does any of the following is guilty of an offense against intellectual property and may be sentenced to imprisonment for not more than five years or to payment of a fine of not more than $5,000, or both:

(1) Modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network; or

(2) Destroys data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network; or

(3) Discloses or takes data, programs, or supporting documentation which is a trade secret within the meaning of Minnesota Statutes, Section 609.52, or is confidential as provided by law residing or existing internal or external to a computer, computer system, or computer network.

Sec. 3. [609.863] [OFFENSE AGAINST INTELLECTUAL PROPERTY INVOLVING FRAUD.] Whoever commits an offense against intellectual property as specified in section 2 for either of the following purposes may be sentenced to imprisonment for not more than 15 years or to payment of a fine of not more than $15,000, or both:

(1) Devising or executing any scheme or artifice to defraud; or

(2) Obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises.

Sec. 4. [609.864] [OFFENSE AGAINST COMPUTER EQUIPMENT OR SUPPLIES.] Whoever intentionally and without authorization modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network is guilty of an offense against computer equipment or supplies and may be sentenced to imprisonment for not more than one year or to payment of a fine of not more than $1,000.

Sec. 5. [609.865] [OFFENSE AGAINST COMPUTER EQUIPMENT OR SUPPLIES INVOLVING FRAUD.] Whoever commits an offense against computer equipment or supplies as specified in section 4 for either of the following purposes may be sentenced to imprisonment for not more than five years or to payment of a fine of not more than $5,000, or both:

(1) Devising or executing any scheme or artifice to defraud; or

(2) Obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises.

Sec. 6. [609.866] [AGGRAVATED OFFENSE AGAINST COMPUTER EQUIPMENT OR SUPPLIES.] Whoever intentionally and without authorization destroys, takes, injures, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network or destroys, injures, or damages any computer, computer system, or computer network is guilty of an aggravated offense against computer equipment or supplies and may be sentenced as follows:

(1) To imprisonment for not more than 15 years or to payment of a fine of not more than $15,000, or both if the damage to the computer equipment or supplies or to the computer, computer system, or computer network is $1,000 or greater, or if there is an interruption or impairment of governmental operation or public communication, transportation, or supply of water, gas, or other public service, or

(2) To imprisonment for not more than five years or to payment of a fine of not more than $5,000, or both if the damage to the computer equipment or supplies or to the computer, computer system, or computer network is greater than $200 but less than $1,000.

(3) In all other cases where the damage to the computer equipment or supplies or to the computer, computer system, or computer network is $200 or less, to imprisonment for not more than one year or to payment of a fine of not more than $1,000.

Sec. 7. [609.867] [OFFENSE AGAINST COMPUTER USERS.] Whoever intentionally and without authorization does either of the following is guilty of an offense against computer users and may be sentenced to imprisonment for not more than five years or to payment of a fine of not more than $5,000, or both:

(1) Accesses or causes to be accessed any computer, computer system, or computer network;

(2) Denies or causes the denial of computer system services to an authorized user of the computer system services, which, in whole or part, is owned by, under contract to, or operated for, on behalf of, or in conjunction with, another.

Sec. 8. [609.868] [OFFENSE AGAINST COMPUTER USERS INVOLVING FRAUD.] Whoever commits an offense against computer users as specified in section 7 for either of the following purposes may be sentenced to imprisonment for not more than 15 years or to payment of a fine of not more than $15,000, or both:

(1) Devising or executing any scheme or artifice to defraud; or

(2) Obtaining money, property, or services by means of false or fraudulent pretenses, representations, or promises.

Sec. 9. This act is effective August 1, 1979 and applies to all crimes committed on or after that date.

MISSOURI

FIRST REGULAR SESSION

[PERFECTED]

SENATE BILL NO. 230

80TH GENERAL ASSEMBLY

INTRODUCED BY SENATORS MURRAY AND CASKEY.

Pre-filed December 1, 1978, and 1,000 copies ordered printed.

Read 2nd time January 8, 1979, and referred to the Committee on Criminal Jurisprudence and Corrections.

Reported from the Committee January 30, 1979 with recommendation that the bill do pass.

Taken up for Perfection March 29, 1979. Bill declared Perfected and Ordered Printed.

VINITA E. RAMSEY, Secretary.

AN ACT

Relating to computers, computer systems, computer networks and computer equipment and supplies, with penalty provisions.

Be it enacted by the General Assembly of the State of Missouri, as follows:

Section 1. Unless the language or context clearly indicates a different meaning is intended, the following words or phrases for the purposes of Sections 2 through 4 shall be given the meaning ascribed to them:

(1) "Access" means to approach, instruct, communicate with, store data, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network.

(2) "Computer" means an internally-programmed, automatic device that performs data processing.

(3) "Computer network" means a set of related, remotely connected devices and communication facilities including more

than one computer system with capability to transmit data among them through communication facilities.

(4) "Computer program" means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data.

(5) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.

(6) "Computer system" means a set of related, connected or unconnected, computer equipment, devices, or computer software.

(7) "Computer system services" means providing a computer system or computer network to perform useful work.

(8) "Financial instrument" means any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card, or marketable security.

(9) "Intellectual property" means data including programs.

(10) "Property" means anything of value as defined in Section 570.010 (10) RSMo, and includes, but is not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

Section 2. 1. A person commits the crime of an offense against intellectual property if he knowingly and without authorization:

(1) modifies data, programs, or supporting documentation residing or existing internal or external to a computer, computer system, or computer network; or

(2) destroys data, programs or supporting documentation residing or existing internal or external to a computer, computer system, or computer network; or

(3) discloses or takes data, programs, or supporting documentation which is confidential as provided by law, or which is a trade secret, residing or existing internal or external to a computer, computer system, or computer network.

2. Offense against intellectual property is a Class D felony, unless the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property, in which case offense against intellectual property is a Class C felony.

Section 3. 1. A person commits the crime of an offense against computer equipment or supplies if he knowingly and without authorization:

(1) modifies equipment or supplies used or intended to be used in a computer, computer system, or computer network; or

(2) destroys, takes, injures or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; or

(3) destroys, injures or damages any computer, computer system, or computer network.

2. Offense against computer equipment or supplies is a Class A misdemeanor, unless:

(1) the offense is committed for the purpose of executing any scheme or artifice to defraud or obtain any property, in which case it is a Class D felony; or

(2) the damage to such computer equipment or supplies or to the computer, computer system, or computer network is greater than $200.00 but less than $1,000.00, in which case it is a Class D felony; or

(3) the damage to such computer equipment or supplies or to the computer, computer system, or computer network is $1,000.00 or greater or if there is an interruption or impairment of a governmental operation or of public communication, transportation, or supply of water, gas, electricity, or other essential public services, in which case it is a Class C felony.

Section 4. 1. A person commits the crime of an offense against computer users if he knowingly and without authorization:

(1) Accesses or causes to be accessed any computer, computer system, or computer network, or

(2) Denies or causes the denial of computer system services to an authorized user of such computer system services, which, in whole or in part, is owned by, under contract to, or operated for, or on behalf of, or in conjunction with another.

2. Offense against computer users is a Class D felony unless the offense is committed for the purpose of devising or executing any scheme or artifice to defraud or to obtain any property in which case an offense against computer users is a Class C felony.

NORTH CAROLINA

GENERAL ASSEMBLY OF NORTH CAROLINA
SESSION 1979

S

2

SENATE BILL 397
Second Edition Engrossed 3/22/79

Short Title: Computer-Related Crime. (Public)

Sponsors: Senator Barnes.

Referred to: Judiciary III.

March 8, 1979

A BILL TO BE ENTITLED

AN ACT TO ESTABLISH A NEW ARTICLE IN CHAPTER 14, CRIMINAL LAW, TO CONTROL COMPUTER-RELATED CRIME.

The General Assembly of North Carolina enacts:

Section 1. Chapter 14 of the General Statutes is amended by adding a new Article to read as follows:

"Article 60.

"Computer-Related Crime.

"§ 14-448. Definitions.--As used in this section, unless the context clearly requires otherwise, the following terms have the meanings specified:

(1) 'access' means to approach, instruct, communicate with, cause input, cause output, or otherwise make use of any resources of a computer, computer system or computer network.

(2) 'computer' means an internally programmed, automatic device that performs data processing.

(3) 'computer network' means the interconnection of communication systems with a computer through

remote terminals, or a complex consisting of two or more interconnected computers.

(4) 'computer program' means an ordered set of data that are coded instructions or statements that when executed by a computer cause the computer to process data.

(5) 'computer software' means a set of computer programs, procedures and associated documentation concerned with the operation of a computer system.

(6) 'computer system' means a set of related, connected or unconnected computer equipment and devices.

(7) 'financial statement' includes but is not limited to any check, draft, money order, certificate of deposit, letter of credit, bill of exchange, credit card of marketable security, or any electronic data processing representation thereof.

(8) 'property' includes but is not limited to, financial instruments, information, including electronically processed or produced data, and computer software and programs in either machine or human readable form, and any other tangible or intangible item of value.

(9) 'services' includes, but is not limited to, computer time, data processing and storage functions.

"§ 14-449. Accessing computers.--(a) A person is guilty of a felony if he willfully, directly or indirectly, accesses or

causes to be accessed any computer, computer system, computer network, or any part thereof, for the purpose of:

(1) devising or executing any scheme or artifice to defraud, or

(2) obtaining property or services for himself or another, by means of false or fraudulent pretenses, representations or promises.

(b) Any person who willfully and without authorization, directly or indirectly, accesses [S-or causes to be accessed] any computer, computer system, computer network, or any part thereof, [S-for any purpose other than those set forth in subsection (a) above,] is guilty of a misdemeanor.

"§ 14-450. Damaging computers and related materials.--A person is guilty of a felony if he willfully and without authorization, alters, damages or destroys:

(a) a computer, computer system, computer network, or any part thereof, or

(b) any computer software, program or data residing or existing internal or external to a computer, computer system or computer network[S-/ or][S-.]

[S-/[illegible]/]

"§ 14-451. Denial of computer services to an authorized user.--Any person who willfully and without authorization denies or causes the denial of computer system services to an authorized user of such computer system services, is guilty of a misdemeanor.

"§ 14-452. Extortion.--Any person who verbally or by a written

or printed communication, maliciously threatens to commit an act described in G.S. 14-450 with the intent to extort money or any pecuniary advantage, or with the intent to compel any person to do or refrain from doing any act against his will, is guilty of a felony."

Sec. 2. This act shall become effective 90 days after ratification.

TENNESSEE

Prefiled for introduction on 1/9/79

SENATE BILL NO. 172

by

Henry

AN ACT making the unauthorized use of computer equipment illegal and to provide penalties for the violation of this Act.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF TENNESSEE:

SECTION 1. It shall be unlawful for any person to knowingly make an unauthorized use of any computer, computer related equipment, operating systems, programmed systems or computer time. Any person violating the provisions of this section shall be guilty of a misdemeanor and upon conviction thereof shall be punished by a fine of not less than five hundred dollars ($500), and, in the discretion of the court, sentenced to not more than six (6) months in jail.

SECTION 2. It shall be unlawful to use any computer related equipment, operating systems, programmed systems, computer time or data stored on computer media with the intent of perpetrating a fraud or a theft by the use of such materials. Any person violating the provisions of this section shall be guilty of a felony and upon conviction thereof shall be subject to a fine of not less than one thousand dollars ($1000) nor more than ten thousand dollars ($10,000) and shall be confined in the state penitentiary for not less than one (1) year nor more than five (5) years.

SECTION 3. This Act shall take effect upon passage, the public welfare requiring it.

Appendix D
OCCUPATIONS AND THEIR RISKS IN COMPUTER TECHNOLOGY

Appendix D

OCCUPATIONS AND THEIR RISKS IN COMPUTER TECHNOLOGY

Seventeen occupations in computer technology are described here in terms of their skills, knowledge, and access to do harm and cause loss. These occupational descriptions also apply to managers of people in these occupations who have the same capabilities as their employees.

USER TRANSACTION AND DATA ENTRY OPERATOR

Function. Operates a remote terminal, enters transactions, data, and programs, at the direction of user personnel.

Knowledge. Source document content and format, terminal output content and format, terminal protocol, identification/verification procedure, other procedural controls.

Skills. Typing and keyboard operation, manual dexterity for equipment operation, basic reading.

Access. Terminal area, source documents, terminal output, terminal operation instructions, identification/verification materials.

Vulnerability. The enterprise is vulnerable to both physical and operational violations by this individual. The principal area of vulnerability is violations that involve the modification, destruction, or disclosure of data belonging to the individual's immediate user organization either internal or external to the system. Two secondary areas of vulnerability are the destruction or disclosure of the user organization's application programs either internal or external to the system and the physical destruction or taking of terminal equipment.

Conclusions. This individual is in a key position relative to the immediate user organization's data and programs entering the system and results exiting the system. Modification of data is considered more of a vulnerability than modification of programs since this individual is not apt to understand enough about the programs to do significant modification damage. A serious danger is that data or programs will be destroyed. If this involves the destruction of source documents for which there is no backup, then it is particularly serious. A mitigating factor is that any individual operator will be able to manipulate data and programs for only those application areas that he normally services.

COMPUTER OPERATOR

Function. Operates a computer from the computer console, alters job schedules and priorities through the console, initiates utility program execution, responds to system error conditions according to documented instructions, mounts magnetic tapes and disk packs, powers up and powers down the system.

Knowledge. Operating system functions, utility program functions, computer processing workflow, system accounting procedures, console protocol, privileged access procedures, physical access procedures.

Skills. Typing and console operation, computer equipment operation, reading procedural documentation, reading and interpreting console messages.

Access. Computer operations area, computer equipment area, files stored in operations area, procedural documentation, privileged access to the computer system.

Vulnerability. The enterprise is vulnerable to both physical and operational violations from this individual. A general area of vulnerability is violations involving the destruction or disclosure of data, application programs, or systems programs internal to the system in main memory or on tape or disk. Other areas include violations affecting system service such as unauthorized use of services, those involving the physical manipulation of system equipment, and destruction or disclosure of data stored external to the system.

Conclusions. This individual is in a key position relative to data and programs internal to the system. Although limited to console operations and programs already in the system, in the absence of other controls, a clever individual in this position would be likely to be able to gain access to any data file or program for the purpose of destruction or disclosure. This individual is also in the position to modify some data. This is restricted to system data, however, not applications data.

PERIPHERAL EQUIPMENT OPERATOR

Function. Operates all equipment immediately peripheral to the computer system having to do with input/output and file usage including card readers, paper tape readers, MICR readers, optical readers, tape drives, disk drives, sorters, tape cleaners, printers, card punches, paper tape punches, COM devices; loads and unloads removable media including punch cards, tape, disk packs, printer listings; installs expendable supplies on the equipment; sorts and labels output.

Knowledge. Computer processing work flow, system accounting procedures, media library, physical access procedures.

Skills. Peripheral equipment operation, reading procedural documentation.

Access. Peripheral equipment area, job setup area, user output distribution area, input data, output results, procedural documentation, expendable supplies.

Vulnerabilities. The enterprise is vulnerable to both physical and operational violations from this individual. The principal area of vulnerability is violations involving destruction or disclosure of data, application and systems programs external to the system but in the general operations area. A secondary vulnerability possiblity has to do with destruction or taking of equipment or supplies.

Conclusions. Although this individual will have access to much input data and output results, the physical situation is likely to be such that copying this information for the purpose of disclosure will be difficult. Certainly it will be somewhat easier to destroy such information.

JOB SETUP CLERK

Function. Assembles jobs including data, programs, and job control information and physically places this material into job queues; requests data from media library; handles procedures for reruns and extraordinary user requests; may also distribute output results.

Knowledge. Computer processing workflow, system accounting procedures, media library, physical access procedures.

Skills. Reading job related documentation, manual capabilities to handle punch cards and magnetic tapes.

Access. Job setup area, user output distribuion area, input data, procedural and data base documentation, may also have access to some media storage and other off-line files.

Vulnerabilities. The enterprise is vulnerable to both physical and operational violations from this individual. The principal area of vulnerability is violations involving destruction or disclosure of data or application programs, external to the system but in the general operations area. A secondary vulnerability is destruction or taking of media; a tertiary and remote possibility is the taking of system service.

Conclusions. Although this individual will have access to much input data and many application programs, the physical situation is likely to be such that copying this informaion for the purpose of disclosure will be difficult. Certainly it will be somewhat easier to destroy such information. As mentioned above, the possibility of the individual taking system service exists but is very remote due to his lack of knowledge as to how the system works.

DATA ENTRY AND UPDATE CLERK

Function. Adds, changes, or deletes records in data bases by means of on-line terminal entry, manual updates to punch card decks, or manual entries on data input forms.

Knowledge. Data base concepts; data base languages; data base files, formats, and content; security access controls; terminal protocol; identification/verification procedure; to some extent, computer processing workflow.

Skills. Typing and terminal or keypunch operation, reading procedural documentation.

Access. Terminal area, data source documents, terminal operation instructions, identification/verification materials, on-line files, documentation on data base structure and content, procedural documentation.

Vulnerabilities. The enterprise is vulnerable to physical and operational violations by this individual. The principal area of vulnerability is violations that involve the destruction or disclosure of data, application programs, or systems programs either internal or external to the system. In addition, this individual has the opportunity to modify data either internal or external to the system and to commit violations having to do with destruction and taking of terminal equipment.

Conclusions. This individual is in a key position relative to data entering the system. Different from many positions, this individual is able to modify the data as well as destroy and disclose. The danger of external manipulation of data is somewhat less than that for internal since it is likely that not all files will be updated by this clerk.

MEDIA LIBRARIAN

Function. Files, retrieves, and accounts for off-line storage of data and programs on tape and other removable media; provides media to production control and job setup areas; cycles backup files to remote facilities.

Knowledge. File names and labels, library and job accounting procedures, computer processing workflow, physical access procedures, archived files.

Skills. Reading procedural documentaion, record keeping and filing.

Access. Tape library, current and aging program and data files, interface to off-site remote storage facilities and to production control.

Vulnerabilities. The enterprise is vulnerable to physical violations from this individual. The principal area of vulnerability is violation involving the destruction or disclosure of data or programs stored external to the system on removable media. A secondary area is violations involving the destruction or taking of the media.

Conclusions. Lack of knowledge as to the content of the files being handled limits the likelihood of fraud by this individual. Physical manipulation of the media with the intent to vandalize is more likely.

SYSTEMS PROGRAMMER

Function. Designs, develops, installs, documents, and maintains operating system and utility software, including programming language compilers, loaders, linkage editors, input/output routines, storage management software, program library access and maintenance routines, terminal and communication line handlers, system debugging facilities, system access controls, job scheduling routines, system accounting facilities, interrupt and trap servicing software, sorting and mathematical utility programs.

Knowledge. Operating systems, programming languages, terminal and computer console protocols, identification/verification procedures, computer processing workflow, hardware system architecture, elementary mathematical functions, boolean algebra, number systems, alphanumeric codes.

Skills. Programming and documentation, computer and peripheral equipment operation, reading and analyzing memory dumps and flowcharts, general diagnostic analysis.

Access. System programming area, system documentation, privileged access to the computer and data communications systems.

Vulnerabilities. The enterprise is vulnerable to physical, operational and programming violations by this individual. A principal area of vulnerability is violations that involve the destruction or disclosure of data, application programs, or systems programs internal to the system in main memory or on tape and disk either by direct, real-time actions or through modification of system software. In addition, this individual is able to modify systems programs internal to the system and to modify, destroy, or disclose systems programs external to the system. Another major area of vulnerability is violations that make unauthorized use or deny authorized use of system services. A secondary area is violations that involve the destruction or taking of terminal equipment.

Conclusions. This individual is in a position to attempt violations in a number of areas and the categories of safeguards mentioned above are apt to have less than total effectiveness in dealing

with a clever systems programmer. Also, all safeguards implemented in software may have limited value since systems programmers are responsible for the design, implementation, and maintenance of such software, and have privileged access to the system. It should be noted that this threat of destruction of system programs external to the system is not so serious since most of them would be backed up with copies on the system.

APPLICATION PROGRAMMER

Function. Designs, develops, installs, documents, and maintains application programs and systems using a variety of programming languages.

Knowledge. Programming languages, EDP procedures and concepts, terminal protocols, identification/verification procedures, elementary mathematical functions, number systems, alphanumeric codes.

Skills. Programming and documentation, programming terminal operation, reading and analyzing memory dumps and flowcharts, general diagnostic analysis.

Access. Application programming area, application programs and their documentation.

Vulnerabilities. The enterprise is vulnerable to physical, operational and programming violations by this individual. A principal area of vulnerability is violations that involve the modification, destruction or disclosure of application programs either internal or external to the system. The individual may also modify, destroy, or disclose the parametric data for his programs. A secondary area of vulnerability is violations that involve the destruction of terminal equipment.

Conclusions. This individual has limited accessibility to areas and facilities that would enable him to attempt violations. Essentially, all he has access to is application programs and just the fraction of those that he is involved with. Conversely, his role with respect to these application programs is such that it is very difficult to be sure that safeguards against his violations will be effective.

TERMINAL ENGINEER

Function. Tests, diagnoses, repairs, replaces, assembles and disassembles terminals or their components.

Knowledge. Electronic, mechanical, and communication engineering; digital logic design; physical access procedures; boolean algebra.

Skills. Operation of terminals and electronic test equipment, reading circuit schematics and diagnostic manuals.

Access. Terminals and adjacent facilities, network diagram, procedural documentation.

Vulnerabilities. The enterprise is vulnerable to physical, operational, and engineering violations by this individual. The principal and only area of serious vulnerability is violations that involve the modification, destruction, or taking of terminal equipment.

Conclusions. Although allowing a well-trained person access to a terminal would appear to pose a multifaceted threat to system security, the only true vulnerability is to physical manipulation of terminal equipment.

COMPUTER SYSTEMS ENGINEER

Function. Tests, diagnoses, repairs, replaces, assembles, and disassembles computer system hardware and components including computers, terminals, peripheral devices, and communication equipment.

Knowledge. Electronic, mechanical, and communication engineering, programming languages, digital logic design, terminal protocols, physical access procedures, boolean algebra.

Skills. Operation of terminals, computer consoles, peripheral devices, communication equipment, and electronic test equipment, programming and documentation, reading and analyzing memory dumps and flowcharts, reading circuit schematics and diagnostic manuals, general diagnostic analysis.

Access. All equipment and adjacent facilities, some system programs with documentation, documentation for all equipment, procedural documentation.

Vulnerabilities. The enterprise is vulnerable to physical, operational, programming, and engineering violations by this individual. The two principal areas of vulnerability are violations that involve the modification, destruction, or taking of system equipment and those that involve unauthorized use or denial of authorized use of system service. A secondary area is violations that involve modification, destruction, of disclosure of system programs internal to the system.

Conclusions. This individual poses as great a threat as anyone in the installation to physical abuse of system equipment and manipulation of system service. Although he might appear to have ready access to other sensitive areas as well, it is possible to effect controls to minimize the vulnerability in these other areas.

COMMUNICATION ENGINEER/OPERATOR

Function. Tests, diagnoses, repairs, replaces, assembles and disassembles, operates data communications equipment including concentrators, multiplexors, modems, and line switching units. Reconfigures communication network when necessary.

Knowledge. Electronic and communication engineering, data communication, terminal protocols, identification/verification procedures, physical access procedures, boolean algebra.

Skills. Operation of terminals, communication equipment, and electronic test equipment, reading circuit schematics and diagnostic manuals, reading procedural documentation.

Access. Communication equipment and adjacent facilities, circuit and network diagrams, procedural documentation.

Vulnerabilities. The enterprise is vulnerable to physical, operational, and engineering violations by this individual. The principal area of vulnerability is violations that involve the destruction or disclosure of data that is internal to the system and is being transmitted in the communication system. A secondary area is violations that involve the modification, destruction, or taking of terminal or communication equipment.

Conclusions. Although this individual is in a position to intercept data for later disclosure, he is not likely to have enough knowledge about the data files to be able to make a judicious selection of material to disclose. The threat from this individual is greater in the area of malicious acts that would serve to disrupt computer processing such as destruction of data files or manipulation of terminal or communication equipment.

FACILITIES ENGINEER

Function. Inspects, adjusts, diagnoses, repairs, replaces, assembles and disassembles equipment supporting computer and terminal equipment, such as power, water, light, heat, and air conditioning equipment.

Knowledge. Electrical and mechanical engineering, physical access procedures.

Skills. Use of test equipment, reading building, circuit, and engineering schematics, reading diagnostic manuals.

Access. All building areas, building and support equipment diagrams and documentation.

Vulnerabilities. The enterprise is vulnerable to physical violations by this individual. The two principal areas of vulnerability are violations that involve denial of authorized system service and destruction or taking of system equipment. A minor area is the modification of system support equipment.

Conclusions. This individual's authorized access to all areas makes him a prime candidate for malicious acts that would serve to disrupt system operation. Similarly, he has greater opportunity than most individuals to take system and system support equipment. Also, due to his authorized access, it is not likely that prevention safeguards will be very effective in his case.

OPERATIONS MANAGER

Function. Designs, develops, installs, modifies, documents, maintains, and manages the computer processing workflow system through direction given to operational subordinates. He is also responsible for physical security of system equipment, and data and programs on removable media stored in the operations area. He may be the assigner of terminal and facilities access control passwords.

Knowledge. Computer processing workflow system, hardware configuration architecture, operations procedures for data files, media storage, job accounting, physical access, and system integration and maintenance, operating system and utility software.

Skills. Developing and reading flowcharts, principles of operation manuals, and other procedural documentation, performing systems analysis and general diagnostic analysis, management.

Access. Computer and peripheral equipment facilities, job input/output, scheduling, and servicing areas, tape library and its media contents, system documentation and all procedural documentation, data files, application programs, and systems programs internal to the system.

Vulnerabilities. The enterprise is vulnerable to physical and operational violations by this individual. There are several areas of serious vulnerability to actions by this individual. Primary areas are the destruction or disclosure of data, application programs, or systems programs internal to the system, destruction or taking of system equipment and unauthorized use or denial of authorized use of system services. In addition, this individual is in a position to destroy or disclose those data files, application programs, and system programs that are stored in the tape (or media) library, and he can modify parametric data either internal or external to the system.

Conclusions. As mentioned above, this individual is in a position to attempt many categories of violations. Also, many of the safeguards against his possible violations are the responsibility of the DP

Department of which he is a key member. Fortunately, with the perferred organization of the DP Department, there is a System Control Group on the same level as this individual's Operations Group. Almost all safeguards of the DP Department that are intended to thwart serious violations by this individual are the responsibility of the System Control Group or the DP Department headquarters. It should be noted that the destruction of system programs external to the system by this individual is not so serious since most of these programs are likely to be backed up in the system.

DATA BASE ADMINSTRATOR

Function. Responsible for adding, changing, and deleting records in on-line and off-line data bases.

Knowledge. Data base concepts, data base languages, data base files, formats, and content, computer processing workflow, security access controls, terminal protocol, identification/verification procedure.

Skills. Typing and terminal operation, reading procedural documentation, performing general diagnostic analysis.

Access. Terminal area, tape (or media) library in the operations area, on-line files, data souce documents, documentation on data base structure and content, procedural documentation.

Vulnerabilities. The enterprise is vulnerable to physical and operational violations by this individual. There are two areas of serious vulnerability to actions by this individual. He has internal and external access to all data that are maintained by the DP Department and since one of his charters is responsibility for modifying these files, the operation is vulnerable to modification of data as well as to destruction and disclosure. A secondary area of vulnerability is violations that involve destruction or taking of terminal equipment.

Conclusions. With the proper organization of the DP Department, this individual will not be administering safeguards that are designed to thwart his violations. The nature of his responsibility, to modify and make corrections to all files, makes detecting his violations particularly difficult.

PROGRAMMING MANAGER

Function. Designs, develops, installs, documents, and maintains application programs through direction given to subordinates.

Knowledge. Programming languages, EDP procedures and concepts, application subject areas, advanced programming and software engineering techniques, data base design procedure, terminal protocol, identification/verification procedures, computer processing workflow, elementary mathematical functions, number systems, alphanumeric codes.

Skills. Programming and documentation, terminal operation, reading and analyzing memory dumps and flowcharts, systems and general diagnostic analysis, management.

Access. Application programming area, application programs and their documentation.

Vulnerabilities. The enterprise is vulnerable to physical, operational, and programming violations by this individual. A principal area of vulnerability is violations that involve the modification, destruction or disclosure of application programs either internal or external to the system. The individual may also modify, destroy, or disclose parametric data for the programs he is responsible for. A secondary area of vulnerability is violations that involve the destruction or taking of terminal equipment.

Conclusions. This individual has limited accessibility to areas and facilities that would enable him to attempt violations. Essentially, he only has access to the application programs generated and maintained by his group. Conversely, his role with respect to the development of these application programs is such that it is very difficult to be sure that safeguards against his actions will be effective.

SECURITY OFFICER

Function. Plans, implements, installs, operates, maintains, and evaluates physical, operational, technical, procedural, and personnel-related safeguards and controls.

Knowledge. Security (including identification) concepts, EDP software and hardware technology, industrial security products, procedural, operational, and personnel policies and practices.

Skills. A level of electronic, mechanical, and programming skills sufficient to allow him to conceive and implement suitable safeguards, reading building, circuit, and engineering schematics, reading diagnostic manuals, reading and analyzing memory dumps and flowcharts.

Access. Privileged access to all areas and all system functions.

Vulnerabilities. The enterprise is vulnerable to all manner of violations by this individual.

Conclusions. There is virtually no possibility of detecting violations perpetrated by individuals in this position. In practice, the individual will often have insufficient knowledge and skills to attempt unauthorized acts in some of the violation areas.

EDP AUDITOR

Function. Performs operational, software, and data file reviews to determine integrity, adequacy, performance, security, and compliance with organizational and generally accepted policies, procedures, and standards; participates in design specification of applications to assure adequacy of controls; performs data processing services for auditors.

Knowledge. Audit techniques, controls, safeguards, system design, software organization, computer applications, facilities security.

Skills. Use of audit tools, programming and documentation, reading technical, operational, and procedural documentation, general diagnostic analysis.

Access. Privileged access to all areas and all system functions.

Vulnerabilities. All manner of violations are possible by this individual.

Conclusions. There is virtually no possibility of detecting violations perpetrated by individuals in this position. All avenues--screening by external CPA auditors, screening by examiners from regulatory agencies, and peer review of the individual's work and activities--should be used to ascertain that the candidate is competent and trustworthy.

Appendix E
AUDIT TOOLS AND TECHNIQUES

APPENDIX E

AUDIT TOOLS AND TECHNIQUES

This appendix contains descriptions of 15 audit tools and techniques. A list of EDP occupations that could be affected follows each description. These are the occupations of people whose errors or criminal acts might be detected by these tools or techniques.

TEST DATA METHOD

The test data method verifies processing accuracy of computer application systems by executing these systems by the use of specially prepared sets of input data that produce preestablished results. The method gives internal auditors a procedure for the verification of computer programs and applications. It is a method that can be used by internal auditors when testing specified and limited program functions. It is a good technique to use initially in program verification because tests can be expanded incrementally. Special procedures are not usually required. The test data method is limited to computer processing verification and evaluation and is not an appropriate technique for verification of production data. No evidence is provided concerning the completeness or accuracy of production input data or master files. The test data method affects the following occupations:

Computer operator	Systems engineer
Peripheral operator	Communications engineer
Job setup clerk	Network manager
Systems programmer	Operating manager
Application programmer	Programmer manager

BASE-CASE SYSTEM EVALUATION

Base-case system evaluation (BCSE) is a technique that applies a standardized body of data (input, parameters, and output) to the testing of a computer application system. This body of data, the base case, is established by user personnel, with internal audit concurrence, as the criterion for correct functioning of the computer application system. This testing process is most widely used as a technique for validation of production computer application systems. One major manufacturing company, however, used the base-case approach as a "means to test programs during their development, to demonstrate the successful operation of the system prior to its installation, and to verify its continuing accurate operation during its life." As such, this approach represents a total commitment by corporate management and each user department to the principles and disciplines of BCSE. The BCSE affects the following occupations:

Computer operator	Systems engineer
Peripheral operator	Communications engineer
Job setup clerk	Network manager
Systems programmer	Operations manager
Applications programmer	Programming manager

INTEGRATED TEST FACILITY

Integrated test facility (ITF) is a technique to review those functions of an automated application that are internal to the computer. Internal auditor's test data are used to compare ITF processing results to precalculated test results. The method is most frequently used to test and verify large computer application systems when it is not practical to separately cycle test data. The ITF technique is used for computer processing verification and evaluation and is of limited value for the verification of production data or data files. Limited evidence is provided concerning the completeness and accuracy of production input data or masterfiles. ITF affects the following occupations:

Communications operator	Systems engineer
Systems programmer	Programming manager
Application programmer	

PARALLEL SIMULATION

Parallel simulation is the use of one or more special computer programs to process "live" data files and simulate normal computer application processing. Whereas the test data method and the ITF process test data through "live" programs, the parallel simulation method processes "live" data through test programs. Parallel simulation programs include only the application logic, calculations, and controls that are relevant to specific audit objectives. As a result, simulation programs are usually much less complex than their application program counterparts. Large segments of major applications that consist of several computer programs can often be simulated for audit purposes with a single parallel simulation program. Parallel simulation permits the internal auditor to independently verify complex and critical application system procedures. Parallel simulation affects the following occupations:

Computer operator	Systems engineer
Peripheral operator	Communications engineer
Communications operator	Network manager
Systems programmer	Operations manager
Applications programmer	Programming manager

TRANSACTION SELECTION

The transaction selection audit technique uses an independent computer program to monitor and select transactions for internal audit review. The method enables the internal auditor to examine and analyze transaction volumes and error rates and to statistically sample specified transactions. Transaction selection audit software is totally independent of the production computer application system and is generally parameter-controlled. No alteration to the production computer application system is required. This technique is especially suitable for noncontinuous monitoring and sampling of transactions in complex computer application systems. Transaction selection affects the following occupations:

Transaction operator	Communication engineer
Peripheral operator	Network manager
Data entry and update clerk	Operations manager
Communications operator	Data base manager
Terminal engineer	Identification control clerk

EMBEDDED AUDIT DATA COLLECTION

Embedded audit data collection uses one or more specially programmed data collection modules embedded in the computer application system to select and record data for subsequent analysis and evaluation. The data collection modules are inserted in the computer application system at points determined to be appropriate by the internal auditor. The internal auditor also determines the criteria for selection and recording. After collection, other automated or manual methods may be used to analyze the collected data.

As distinct from other audit methods, this technique uses "in-line" code (i.e., the computer application program performs the audit data collection function at the same time it processes data for normal production purposes). This has two important consequences for the auditor: in-line code ensures the availability of a comprehensive or a very specialized sample of data (strategically placed modules have access to every data element being processed); retrofitting this technique to an existing system is more costly than implementing the audit programming during system development. Because of this, it is preferable for the internal auditor to specify his requirements while the system is being designed. Embedded audit data collection affects the following occupations:

Transaction operator	Terminal engineer
Computer operator	System engineer
Peripheral operator	Communications engineer
Job setup clerk	Network manager
Data entry and update clerk	Operations manager
Communications operator	Data base manager
	Identification control clerk

EXTENDED RECORDS

The extended records technique gathers together by means of a special program or programs all the significant data that have affected the processing of an individual transaction. This includes the accumulation into a single record of results of processing over the time period that the transaction required to complete processing. The extended record includes data from all the computer application systems that contributed to the processing of a transaction. Such extended records are compiled into files that provide a conveniently accessible source for transaction data.

With this technique, the auditor no longer need review several files to determine how a specific transaction was processed. With extended records, data are consolidated from different accounting periods and different computer application systems to provide a complete transaction audit trail physically in one computer record. This facilitates tests of compliance to organization policies and procedures. The extended records technique affects the following occupations:

Transaction operator	Communication engineer
Peripheral operator	Network manager
Data entry and update clerk	Operations manager
System programmer	Data base manager
Application programmer	Programming manager
Terminal engineer	Identification control clerk
Systems engineer	

GENERALIZED AUDIT COMPUTER PROGRAMS

Generalized audit computer programs are the most widely used in techniques for auditing computer application systems. These products permit the internal auditor to independently analyze a computer application system file. Most generalized audit packages, because of their widespread use and long history, are ultrareliable, highly flexible, and extensively and accurately documented. Generalized audit programs currently available can be used to foot, cross-foot, balance, stratify, select a statistical sample, select transactions, total, compare, and perform calculations on diverse data elements contained

within various data files. These extensive capabilities are available to the internal auditor to substantively test computer application systems. Generally, this audit method is used to test computer file data; little facility is present to test system logic, other than implicitly by the results that appear in the data files. No explicit compliance testing facility is contained in these programs. Historically, generalized audit programs are operated only in the batch mode. Recently, with the rapid expansion of on-line computer application systems, on-line generalized audit programs have become available. Use of generalized audit programs affect the following occupations:

Transaction operator	Terminal engineer
Computer operator	System engineer
Peripheral operator	Communication engineer
Job setup clerk	Network manager
Data entry and update clerk	Operations manager
Communications operator	Data base manager
Media librarian	Programming manager
Systems programmer	Identification control clerk
Application programmer	

SNAPSHOT

Both internal auditors and data processing personnel periodically encounter difficulty in reconstructing the computer decisionmaking process. The cause is a failure to keep together all the data elements in that process. Snapshot is a technique that, in effect, takes a picture of the parts of computer memory that contain the data elements in a computerized decisionmaking process at the time the decision is made. The results of the snapshot are printed in report format for reconstructing the decisionmaking process.

The snapshot audit technique offers the capability of listing all the data in a specific decisionmaking process. The technique requires the logic to be preprogrammed in the system. A mechanism, usually a special code in the transaction record, is added to trigger the printing of the data in question for analysis.

The snapshot audit technique helps internal auditors answer questions as to why computer application systems produce questionable results. It provides information to explain why a particular decision was developed by the computer. Snapshot audit used in conjunction with other audit techniques (e.g., integrated test facility or tracing) determines of what results would occur if a certain type of input entered the data processing system. The snapshot audit technique also can be an invaluable aid to systems and programming personnel in

debugging the application system because it can provide snapshots of computer memory as a debugging aid. The snapshot audit affects the following occupations:

System programmer	Communication engineer
Application programmer	Network manager
Terminal engineer	Data base manager
Systems engineer	Programming manager

TRACING

A traditional audit technique in a manual environment is to follow the path of a transaction during processing. For example, an auditor picks up an order as it is received into an organization and follows the flow from work station to work station. The internal auditor asks the clerk involved what actions were taken at that particular step in the processing cycle. Understanding the policies and procedures of the organization, the internal auditor can judge whether they are being adequately followed.

After walking through the processing cycle, the internal auditor has a good appreciation of how work flows through the organization. In a data processing environment, it is not possible to follow the part of a transaction through its processing cycle solely by following the paperwork flow. Many of the functions performed by clerks and the movement of hardcopy documents are replaced by electronic processing of data.

The tracing audit technique provides the internal auditor with the ability to perform an electronic walk-through of a data processing application system. The audit objective of tracing is to verify compliance with policies and procedures by substantiating, through examination of the path through a program that a transaction followed, how that transaction was processed. It can be used to verify omissions. Tracing shows what instructions have been executed in a computer program and in which sequence they have been executed. Because the instructions in a computer program represent the steps in processing, the processes that have been executed can be determined from the results of the tracing audit technique. Once an internal auditor knows what instructions in a program have been executed, an analysis can be performed to determine if the processing conformed to organization procedures. The tracing technique affects the following occupations:

Systems programmer	Communication engineer
Application programmer	Network manager
Terminal engineer	Programming manager
Systems engineer	

MAPPING

Mapping is a technique to assess the extent of system testing and to identify specific program logic that has not been tested. Mapping is performed by a program measurement tool that analyzes a computer program during execution to indicate whether program statemets have been executed. This measurement tool can also determine the amount of CPU time consumed by each program segment.

The original intent of the mapping concept was to help computer programmers ensure the quality of their programs. However, auditors can use these same measurement tools to look for unexecuted code. This analysis can provide the auditor with insight into the efficiency of program operation and can reveal unauthorized program segments included for execution for unauthorized purposes. The mapping method affects the following occupations:

System programmer
Application programmer
Programming manager

CONTROL FLOWCHARTING

In a complex business environment, it is difficult to thoroughly understand the total system of control of an organization within its total business and operational context. A graphic technique, or flowchart, for simplifying the identification and interrelationships of controls can be a great help in evaluating the adequacy of those controls and in assessing the impact of system changes on the overall control profile. Flowcharts facilitate the explanation of controls to a system analyst or external auditor, or to personnel unfamiliar with specific operational systems; they also aid in ascertaining that controls are operating as originally intended.

The audit area control flowchart technique provides the documentation necessary to explain the system of control. Often an organization's information about controls is fragmented. This makes it difficult to obtain a clear picture of the controls operating within the organization. The availability of an overall picture of controls, using several levels of flowcharts, facilitates understanding. Control flowcharting affects the following occupations:

Communications operator	Operations manager
System programmer	Data base manager
Application programmer	Programming manager
Network manager	

JOB ACCOUNTING DATA ANALYSIS

Job accounting facilities are available through most computer vendors as an adjunct to their operating systems. The job accounting facility is a feature of the computer operating system software that provides the means for gathering and recording information to be used for billing customers or evaluating systems usage. Examples of information collected by a job accounting facility are job start and completion times, usage of data sets, and usage of hardware facilities. These job accounting systems were designed by the vendors to serve the operating needs of the data processing department. However, much of the information provided by these facilities is of interest to internal auditors.

Two types of job accounting data, the accounting records and the data set activity records, are of interest to the internal auditor. Accounting records consist of records that show which user used which programs, how often, and for how long. They include an identification of the user, the hardware features required by the job, the time it took to perform the job, and how the job was completed. Data set activity records provide information about which data files were used during processing and who requested the use of the data sets. Among the information contained in these records are the data set name, record length, serial number of the volumes, and the user of the data set.

The internal auditor can use data from the accounting records to verify charges for use of the computer resources. They also enable the auditor to verify that only authorized individuals use the computer. Data set activity records provide the auditor with a means to verify that data are being used by authorized individuals. The job accounting data analysis affects the following occupations:

Transaction operator	Application programmer
Computer operator	Network manager
Peripheral operator	Operations manager
Job setup clerk	Data base manager
Communications operator	Programming manager
Media librarian	Identification control clerk

SYSTEM ACCEPTANCE AND CONTROL GROUP

When the EDP auditor decides to monitor and review the computer application development process, the auditor must determine how to best perform the review. Although the substance of the review is unchanged, the EDP auditor may choose to perform the review personally or to rely on the efforts of another group. To perform the review personally is the choice made by many EDP auditors, even though substantial effort and training may be required to do an effective job. That much of the training required has to do with data processing rather than with EDP

auditing has, among other factors, caused the auditors at a large insurance company to choose another approach. The company has established, in the data processing department, a Systems Acceptance and Control (SAC) Group to perform systematic reviews of computer application system developments and to create and maintain effective computer application system standards, particularly in the area of auditability. The SAC approach affects the following occupations:

System programmer	System engineer
Application programmer	Communication engineer
Terminal engineer	Programming manager

CODE COMPARISON

Code comparison entails comparison of two copies, made at different times, of the program coding for a particular application. The objective of this technique is to verify that program change and maintenance procedures and program library procedures are being followed correctly. The auditor uses the output of the comparison to identify changes that have occurred between the making of the two copies. The auditor then locates and analyzes the documentaion that was prepared to authorize and execute the changes. This technique supports compliance testing rather than substantive testing. Code comparison is especially useful for auditing programs that perform critical business functions and are subject to continuing change. The code comparison technique affects the following occupations:

Computer operator	System engineer
Job setup clerk	Communication engineer
System programmer	Operations manager
Application programmer	Programming manager
Terminal engineer	

Appendix F
TIME-SHARING USAGE EXAMPLES

Appendix F

TIME-SHARING USAGE EXAMPLES

Three examples of the use of nationally known time-sharing services are provided below to show the range of time-sharing features and methods in use.

Table F.1 was copied from an actual time-sharing terminal output listing produced during a session using a time-sharing service. It shows the typical user interaction for this type of computer use. Numerous time-sharing services are available throughout the United States and in other countries. A line-by-line description of the exhibit follows.

Small-case type is produced by the user at a typewriter-like computer terminal. Large-case type is produced by the computer system in response to what the terminal user types, according to the computer program being used at the time. Numbers in parentheses reference lines in the table.

EXAMPLE: EQUIPMENT AND SYSTEM IDENTIFICATION (01-04)

In this interaction sequence, the terminal user interacts with the computer's communication system and identifies the computer equipment and the operating system he desires to use.

(01) The user types the code "ba" in initializing his run, to indicate that he wishes to use the vendor's production computer, and text editing system. He would have typed another 2 digit code if he wished to use different computer equipment and operating system packages available to users. The computer responds to the user's input with a protocol message that serves to identify the communication line desired.

(02) The user once again types "ba" to select the equipment and operating system he wants to use.

(03) The computer responds that the desired system is operating and is ready for the next steps in the log-on process.

(04) The computer then requests the 2-digit code which corresponds to his terminal type. This information is necessary so a translational table may be used that allows different types of terminals to communicate with the same computer system. The terminal user types "aj" which is the manufacturer code for the manufacturer of his computer terminal. Use of an incorrect code will cause communication with the computer system to be garbled and unintelligible.

Table F.1

TIME-SHARING LISTING: EXAMPLE 1

LINE REFERENCE	TERMINAL LISTING	
(01)	baIBUALI SYSTEM ID	EQUIPMENT & SYSTEM IDENTIFICATION
(02)	ba	
(03)	READY	
(04)	MODEL? aj	
(05)	OSI/SUPERWYLBUR: LINE 39 05/23/79 12:25:24 P.M.	LOG-ON AUTHORIZATION
(06)	LIST FROM &PUBLIC.TRAINING FOR JUNE, 1979 TRAINING SCHEDULE	
(07)	TERMINAL? t00	
(08)	ACCOUNT?	
(09)	USER?	
(10)	KEYWORD?	
(11)	ILLEGAL KEYWORD	
(12)	ACCOUNT?	
(13)	USER?	
(14)	KEYWORD?	
(15)	INITIALIZING FROM LAST SESSION	RETRIEVAL FROM FILE
(16)	? clr text	
(17)	? use from samplefile on sri001	
(18)	"SAMPLEFILE" NOT FOUND ON SRI001	
(19)	? use from &sampl***	
(20)	? use from &csa.samplefile on sri001	
(21)	?,list	
(22)	1. THIS IS A SAMPLE FILE. IT MIGHT CONTAIN SENSITIVE INFORMATION 2. OR CONTAIN INSTRUCTIONS FOR THE COMPUTER TO PERFORM SOME 3. RESTRICTED TASKS. IT IS PROTECTED BY SEVERAL CODES. TO READ 4. THIS FILE YOU MUST KNOW THE ACCOUNT NUMBER, THE USER INITIALS, 5. AND THE FILE NAME. TO WRITE ON TOP OF THE FILE YOU MUST 6. ALSO KNOW THE THE KEYWORD ASSOCIATED WITH IT. THIS FILE 7. COULD ALSO HAVE BEEN ENCODED IF THE CREATOR OF THIS FILE 8. HAD SO WISHED. THEN THE READER WOULD HAVE BEEN REQUIRED 9. TO KNOW A CODE WORD ALSO.	
(23)	? insert 10,11,12	
(24)	10. ? THIS LOCAL *** 10. ? I A***	
(25)	10. ? i am changing my personal copy of the file. to change the 11. ? copy of the file used by others i must successfully "resave" 12. ? the file.	
(26)	? l/st	
(27)	1. THIS IS A SAMPLE FILE. IT MIGHT CONTAIN SENSITIVE INFORMATION 2. OR CONTAIN INSTRUCTIONS FOR THE COMPUTER TO PERFORM SOME 7. RESTRICTED TASKS. IT IS PROTECTED BY SEVERAL CODES. TO READ 4. THIS FILE YOU MUST KNOW THE ACCOUNT NUMBER, THE USER INITIALS, 5. AND THE FILE NAME. TO WRITE ON TOP OF THE FILE YOU MUST 6. ALSO KNOW THE THE KEYWORD ASSOCIATED WITH IT. THIS FILE 7. COULD ALSO HAVE BEEN ENCODED IF THE CREATOR OF THIS FILE 8. HAD SO WISHED. THEN THE READER WOULD HAVE BEEN REQUIRED 9. TO KNOW A CODE WORD ALSO.	
(28)	10. I AM CHANGING MY PERSONAL COPY OF THE FILE. TO CHANGE THE 11. COPY OF THE FILE USED BY OTHERS I MUST SUCCESSFULLY "RESAVE" 12. THE FILE.	
(29)	? resave	DATA SECURITY
(30)	KEYWORD FOR 1896-CSS?	
(31)	INCORRECT KEYWORD	
(32)	REQUEST NOT EXECUTED	
(33)	? use from &css.samplefile on sri001	RETRIEVAL FROM FILE
(34)	IF IT'S OK TO CLEAR "&CSS.SAMPLEFILE", REPLY "YES"	
(35)	CLEAR? yes	
(36)	? list	
(37)	1. THIS IS A SAMPLE FILE. IT MIGHT CONTAIN SENSITIVE INFORMATION 2. OR CONTAIN INSTRUCTIONS FOR THE COMPUTER TO PERFORM SOME RESTRICTED TASKS. IT IS PROTECTED BY SEVERAL CODES. TO READ THIS FILE YOU MUST KNOW THE ACCOUNT NUMBER, THE USER INITIALS, AND THE FILE NAME. TO WRITE ON TOP OF THE FILE YOU MUST ALSO KNOW THE THE KEYWORD ASSOCIATED WITH IT. THIS FILE COULD ALSO HAVE BEEN ENCODED IF THE CREATOR OF THIS FILE HAD SO WISHED. THEN THE READER WOULD HAVE BEEN REQUIRED TO KNOW A CODE WORD ALSO.	
(38)	? log-off clean	LOG-OFF
(39)	05/23/79 Wednesday 12:31:09 p.m.	
(40)	$0.31 - CHARGE	
(41)	END OF SESSION	

Log-On Authorization (05-14)

In this interaction sequence, the terminal user interacts with the operating system he specified and identifies himself as an authorized user to gain access to records stored within the computer and to use computer resources.

(05) The software package, SUPERWYLBUR, selected by the user in 02, identifies itself. "Line 39" is identified as the specific communication line the user and computer are connected by, this will serve as a reference for the computer operator should the operator need to directly communicate with the terminal user. The date and time of contact with SUPERWYLBUR also are listed.

(06) This is a systems message. It was initialized by the computer operator at an earlier time and automatically greets users to notify them of upcoming systems changes.

(07) SUPERWYLBUR requests a three-character computer terminal identification code from the user. The terminal ID code is used for billing and could be used to track activity at a specific terminal. The security potential of the terminal ID code is not utilized; no validity check on the codes entered is performed.

(08, 09, 10) The computer prompts: "ACCOUNTS?", "USER?", and "KEYWORD?", are the primary security checks in the SUPERWYLBUR system. To gain access to certain records in the system or to use computer resources, the terminal user must type in a valid 1- to 4-digit account number, a valid 3-digit user code, and a valid 3-digit keyword. For each valid account number, a limited number of user codes are established by the account holder and divulged to the vendor for data processing. Each authorized user is given a user code by the account holder. The terminal user then sets up a secret keyword on his terminal. If an unauthorized user discovers the account number and user codes, which often are not rigorously guarded, he still cannot access the system unless he can obtain the user's unique keyword which corresponds to the account number and user code he has discovered. A series of Ms and Xs are typed one on top of the other, the terminal user types his codes on top of these "underscored" letters which makes the codes unintelligible to the eye.

(11) The keyword typed by the user in (10) was invalid, it did not match the keyword established by the user of the account. The computer indicates this to the terminal user.

(12) After the input of an invalid keyword the computer repeats the three security prompts by first requesting the account number code. The user responds by typing the code over the underscored characters.

(13) The account number code typed by the terminal user was valid--it matched an account number in the computer file. The computer next prompts the user for his user code, which the user types over the underscored characters.

(14) The user code typed by the user was valid--it corresponded to the account number code previously typed. The computer then prompts the user for his keyword, which he types in.

Retrieval from File (15-28)

The terminal user has just effected an authorized log-on. In this series of interactions, the user copies a file from the computer disk to a section of main memory in the CPU and performs list and add operations to the file data.

(15) After his successful log-on, the user is notified by the computer that during his last session he left a file intact within the default working file of the CPU. The computer is ready to perform operations on this file as per the user's instructions.

(16) The question mark indicates the computer is waiting for a command from the user. The user gives the command to clear this "old" text from the default file.

(17) A question mark indicates that the user's request in (16) was completed, and the computer awaits another command. The user asks the computer to bring in the data set called "samplefile," which may be found on the memory disk, volume serial # "SRI 001."

(18) The computer tells the terminal user that a data set called samplefile, on disk SRI 001 available to his user code and account number could not be found.

(19) Prompted by the computer for another command, the user begins to request another dataset, but makes a typing error.

(20) The computer recognizes that a mistake has been made and prompts the user for another command. The user requests the same file, samplefile, in a manner that allows him authorized access to this protected file. The originator of samplefile had declared that samplefile would only be observable to other users who knew his user code, ostensibly a small group of co-workers. Hence, the file named "samplefile" was created as a file type that requires a code--in this case, the user ID code as a prefix to the file name. The terminal user requests "samplefile" and correctly includes the user code prefix in his command.

(21) The question mark acknowledges that samplefile has been found, a copy has been transfered to the main memory, and samplefile is ready for use. The user commands the computer to list the entire file.

(22) The computer lists samplefile as commanded.

(23) Prompted by the computer for another command, the terminal user directs the computer to add 3 lines, lines 10, 11, and 12 to the file. This addition will affect the file only in the main memory, not the file on disk.

(24) The question mark and "10" means the computer acknowledges the command and requests the text for line 10. The user begins typing the text to line 10, but makes a mistake and indicates this by typing three asterisks.

(25) The terminal user types the text for lines 10, 11, and 12.

(26) The question mark produced by the computer indicates that the text to lines 10, 11, and 12 have been added to the copy of samplefile within the main memory. The user commands the computer to list this copy so he can visually verify the addition.

(27) Lines 1-10 are the original samplefile.

(28) Lines 10-12 are the added lines. The user can see that the main memory copy of samplefile includes his addition.

Data Security (29-32)

In this interaction sequence, the user attempts to modify the original copy of samplefile on the disk. To do so, he must comply with the data security checks put on samplefile by its originator.

(29) The user commands the computer to rewrite the altered 12-line file onto the original file copy.

(30) Because it is not his own data set he is altering, the terminal user is prompted to give the keyword that corresponds to the user code of the person who originated samplefile. The computer refers to samplefile by the account number "1896" and the user code, "CSS." In doing so, the account number is openly revealed for the first time, and the user code is openly revealed for the second time [see (20)]. Hence, a perpetrator who came into possession of this terminal listing would need only the secret keyword to gain complete access to samplefile. The terminal user types in a 3-digit keyword over the underscored characters.

(31) The keyword typed by the user does not match the authorized keyword and the computer indicates this.

(32) Because the terminal user did not pass the data security checks required to alter samplefile, the computer did not execute his request to have the 12 line file rewritten onto the original file; the original is preserved intact.

Retrieval from File (33-37)

Once again the user clears his file from the main memory of the CPU and lists a copy of the original file.

(33) The terminal user accesses the original file name "samplefile" on disk volume SRI 001.

(34) however, the user has not told the computer what to do with the 12-line samplefile he created in (20)-(25). Therefore, the computer asks the user to respond by typing "YES," if he wants the 12-line version of samplefile cleared from the main memory.

(35) The user responds affirmatively.

(36) The question mark indicates the previous command has been executed and the computer awaits another command. The terminal user responds by commanding the computer to list samplefile as it appears on disk.

(37) The computer lists samplefile. This listing is identical to the first listing (22); the data security features incorporated within samplefile protected it from modification by an unauthorized person.

Log-Off (38-41)

In this short series of interactions, the user completes his session on the time-sharing system and then receives a summary of accounting data.

(38) The user commands the computer to terminate his session and to erase the data he had called into the main memory of the CPU to work on. This will leave samplefile intact in its original form on disk.

(39) The computer acknowledges that a log-off has been executed by presenting the log-off date, day of week, and time of day.

(40) The computer presents the cummulative charge of the session.

(41) The computer indicates the session is over, and the log-off is complete.

EXAMPLE 2

Table F.2 is another example of services available. The terminal interaction is provid l. A line-by-line description of the exhibit follows.

Table F.2

TIME-SHARING LISTING: EXAMPLE 2

```
Line
Reference                    Terminal Listing
(01)  □                                                  EQUIPMENT IDENTIFICATION
(02)    ONLINE - SUNY
(03)  >L SUNY WPETRO                                     LOG-ON AUTHORIZATION
(04)  PASSWORD:
(05)
(06)  PASSWORD INCORRECT.
(07)  PASSWORD:
(08)
(09)  PASSWORD INCORRECT.
(10)  LOGGED OFF AT 11.48.08 ON 30MAY79
(11)  □                                                  EQUIPMENT IDENTIFICATION
        ONLINE - SUNY
(12)  >L SUNY WPETRO                                     LOG-ON AUTHORIZATION
      PASSWORD:

      PASSWORD INCORRECT.
(13)  PASSWORD:

(14)  A/C INFO:
(15)  *RWH-TEST
(16)  ** ALL CLEVELAND USERS PLZ. TYPE 'INFO CLEMOVE' **
(17)  SUNY READY AT 11.49.36 ON 30MAY79
(18)    .30Z 0!MAY78
                                                         RETRIEVAL FROM FILE
(19)  11.49.43 >L * NOMAD
(20)  FILENAME FILETYPE MODE   ITEMS
(21)  THMMAN1  NOMAD      P      20
      THMMAN2  NOMAD      P      21
      THMMAN3  NOMAD      P      68
      THMMAN   NOMAD      P      20
      THMMAN4  NOMAD      P     110
      EXP1     NOMAD      P      12
(22)  BAL      NOMAD      P       8
      BAL1     NOMAD      P       6
      ART6     NOMAD      P       8
      ART4     NOMAD      P       8

(23)  11.50.22 >E BAL NOMAD
(24)  EDIT:
(25)  >P 40
(26)      QUERY T;
      SELECT PRODCD AMONG(350,580,690);
      SELECT ADD REGNCD='WE' CAPYY=79;
      CREATE BY COUNNM
      BY COMPNM
      BY LOCNM
      ACROSS PRODSN AS A5 SUM(CAPTOT) HEADASIS ON T;
      QUERY T;
(27)  EOF:
(28)  >TOP
(29)  >LOC /BY/
(30)  CREATE BY COUNNM
(31)  >C /BY/QQQ/
(32)  CREATE QQQ COUNNM
(33)  >Q
                                                         DATA SECURITY
(34)  11.51.32  >ATT PETRO
(35)  PASSWORD:
(36)
(37)  PETRO    ATTACHED AS T-DISK
(38)  THE DATABASE IS CURRENTLY BEING UPDATED WITH NEW
      DATA.  THIS PROCESS SHOULD BE FINISHED BY 30MAY79.
      FOR INFORMATION CONCERNING THE ITEMS BEING UPDATED,
      CONTACT SRI INTERNATIONAL. 29MAY79 RCH.
                                                         LOG-OFF
(39)  11.51.42  >LOG
(40)  3.92 ARU'S, .05 CONNECT HRS
(41)  LOGGED OFF AT 11.52.03 ON 30MAY79
      XO-
```

The characters typed by the terminal user are those that are preceeded by the greater than symbol ">". An exception to using this symbol is the user's password.

Equipment Authorization (01-02)

The terminal user has established a telephone communication link with the time-sharing service by dialing the correct telephone number. In the next two interactions, the user identifies his terminal type, and the computer system identifies itself to the user.

(01) The user types a quad symbol (square) which is the character speed code that corresponds to the type of terminal he is using. The code may be obtained from the vendor. It allows the computer to translate messages to suit the terminals speed and formatting characteristics.

(02) The compter indicates that it recognizes the user's terminal when it identifies itself as "ONLINE-SUNY" which means the user has established communication with a computer system in Sunnyvale, California.

Log-On Authorization (03-10)

In this series of interactions, the user must supply an authorized password before he may access computer files and use computer resources.

(03) The "greater than" sign is the computer's prompt to the user. The command typed by the user means he wishes to link into the computer system signified by the 4-digit code "SUNY." "WPETRO" is the user's (1-8 digit) identification code. Note that this code is not concealed by underscoring.

(04) The computer prompts the user for his password.

(05) The computer prints the characters 8, M, and * on top of one another, on eight successive spaces to form underscoring. The user types his 1- to 8-digit password over the underscoring. The presence of the underscoring prevents a potential perpetrator from obtaining the terminal user's password by viewing the computer listing.

(06) The password typed by the user in (05) did not match the authorized password that corresponds to the user name "WPETRO." The computer indicates this.

(07) The computer gives the terminal user a second chance to type the correct password. The user has 28 seconds to type the correct password.

(08) The computer types the underscoring over which the user types the password.

(09) Once again the user typed an incorrect password and the computer indicates this.

(10) If the user fails to type in the correct password on the second attempt, it is assumed that the user does not know the password, and the system is programmed to autmatically log-off. The time and date of log-off are listed.

Equipment Identification (11)

Failure to type the correct password the second time requires the following procedure to be initiated.

(11) Following the automatic log-off, the user reestablishes telephone communication with the service and repeats the equipment identification steps (01-02).

Log-On Authorization (12-18)

(12) Once again, the user types in an invalid password and the computer indicates this. After the user has identified his terminal type and has been greeted by the computer system (11), he repeats the log-on authorization routine which he failed previously (03-10).

(13) The user is given a second chance to type the correct password.

(14) The computer prompt "A/C INFO" indicates the terminal user has typed in the correct password, and he should now type in a title or description of his computer run which will appear on his computerized bill.

(15) The user responds by typing "RWH-TEST." "RWH" are probably his initials, and the word test will remind him when he reads his bill that this was a test run he made.

(16) The computer then printed a systems message that was initiated earlier by the computer operator and that automatically greets each user after the user has successfully logged on. This message probably was in regard to the move by the Cleveland office to a new facility.

(17) The computer's next message means the user has successfully gained access to the Sunnyvale computer system which is ready to execute his commands. The time and date of access are given.

(18) The computer lists the name of the operating system being used--version 302--and the date it was placed in operation.

Retrieval from File (19-33)

In this sequence, the terminal user retrieves a file from a disk in permanent storage and edits the file copy while it is temporarily held in the main storage of the CPU.

(19) The computer lists the time and a "greater than" sign; this indicates the user has full access to the computer, and the computer awaits his first command. The terminal user responds by requesting the computer to list the directory of all his files written in the language called "NOMAD."

(20) The computer first prints the directory heading. "Filename" is the unique name that the user gives to each set of records he establishes. "Filetype" is the language and format type that characterizes the file; other files may be a filetype, such as COBOL. "Mode" is the specific area that belongs to the user and where the file may be found; "P" refers to permanent storage. "Items" are the number of lines in the file. The directory is a preprogrammed feature of the operating system; it automatically updates itself whenever the user establishes or alters a file.

(21) These lines contain the listing of the user's files. The first listing is a file named "THMMANI" of "NOMAD" type, stored in the permanent section of the user's disk and consists of 20 lines.

(22) The file named "BAL" is retrieved by the user in (23).

(23) The user presses the carriage return key of his terminal to indicate he is finished viewing his directory of files. The computer responds by printing the time and prompts the user for another command. The user commands the computer to edit the file named "BAL" of type "NOMAD," (22). Each file must be identified by its name and type, as the user has done.

(24) The computer acknowledges the command and prompts the user for specific editing instructions. The acknowledgement indicates the "BAL" file has been copied from the permanent section of disk to the main storage of the CPU. The file now resides in both permanent (disk) and temporary (core) storage.

(25) The user tells the computer to list (print) the first forty lines of the file.

(26) The computer lists "BAL."

(27) "EOF" stands for end of file and means the entire file has been listed. The computer awaits further editing instructions. The computer listed 8 lines, although the user requested that the first 40 lines of "BAL" be listed. However, as may be seen (22), the "BAL" file only contained 8 items, all of which were listed by the computer.

(28) The user responds to the computer's prompt by commanding that the computer's "pointer" go to the top or first line of the file.

(29) The user then commands the computer to search the entire file and locate the word "BY."

(30) The computer lists the line in which the word "BY" is situated, signifying it has located the word and also giving the user a chance to verify that the computer has located the correct listing of "BY" if it happens to occur more than once in the file.

(31) The user commands the computer to change "BY" to "QQQ."

(32) The computer does this and prints out the modified line for user verification.

(33) The computer requests another command, and the user instructs the computer to "quit." This command deletes the copy of "BAL" in the main storage of CPU. It does not affect the original "BAL" file on disk, which remains unmodified. Had the user typed the word "file," the edited copy of "BAL" would have replaced the original copy on disk. The quit command deletes the altered version of the file held in temporary storage (main storage).

Data Security (34-38)

In this sequence, the user requests that a disk belonging to another user be attached. To access this protected disk the terminal user must know and type the other user's password.

(34) Having quit his edit routine, the user is returned to command level communication with the computer and the time is given. Prompted by the computer, the user commands that the disk belonging to a user code named "PETRO" be attached.

(35) The computer requests the password that correspondes to "PETRO." This data security measure prevents unauthorized users from viewing, modifying, or deleting data held in protected disk files.

(36) The user types the appropriate password over the underscored characters.

(37) The computer's message indicates that the password used was correct and that "PETRO" has been attached as the "T-DISK;" an arbitrary letter T is assigned as a title to "PETRO" to differentiate it from a "P" mode disk which is the user's permanent disk.

(38) The originator of the disk preprogrammed this message to greet users who access his disk.

Log-Off (39-41)

In this sequence of interactions, the user terminates his communication with the computer and the computer presents basic accounting information.

(39) The computer awaits the user's instructions about what to do with "PETRO." The user directs the computer to terminate his session at the terminal by typing LOG.

(40) The computer prints out accounting data. "ARU'S" is an accounting algorithim that lumps CPU and I/O time into one unit figure. Connect hours are listed in hundredths of an hour.

(41) The computer lists that a log-off has been effected and the time and date it has been completed. The stray characters "XO-" are printed after the terminal link has been severed and therefore are not meaningful.

EXAMPLE 3

Finally, a third example of popular time-sharing services is provided in Table F.3, followed by an explanation.
Following the log-on sequence, user commands may usually be identified as those characters preceeded by a greater than sign ">".

Equipment Identification (01, 02, & 06)

By dialing a phone number given to him by the vendor, the user establishes a telecommunication link with the time-sharing service; a high-pitched tone on the receiver is evidence of his contact with the service. After plugging the receiver into his computer terminal or communication modem, the user must identify to the computer network the type of terminal he is using. Correct identification of his terminal type will ensure that no characters are lost in his communication with the computer.

(01) The user presses the carriage return key and is prompted for his terminal identifier code. The prompt indicates he has a positive connection with the computer. The user types the code on the same line as the computer prompt. In this case, the user typed an "E," a code which means that the terminal used has a speed of 30 characters per second. The "E," however, does not appear on the listing.

(02) The computer responds by assigning a location code, "1017", Palo Alto, CA, and a port of entry number, "04", to the communication link. The code aids the vendor's staff in identifying specific user "links" in the event of communication problems.

Table F.3

TIME-SHARING LISTING: EXAMPLE 3

Line Ref.#	Terminal Listing	
(01)	Please Type Your Terminal Identifier	Equipment Identification
(02)	-1017-04--	
(03)	Please Log In: DIST1OE:	
(04)	Error, Type Password:	Log-On Authorization
	Error, Type Password:	
	Error, Type Password:	
(05)	Please See Your Representative	
	If You Are Having Trouble Logging In	
(06)	Please Type Your Terminal Identifier	Equipment Identification
	-1017-04--	
	Please Log In: DIST1OE:	Log-On Authorization
(07)	PROJECT CODE:.LOGOFF AT 11:19:36 PDT TUESDAY 06/19/79 BY SYSTEM	
(08)	Please Log In: DIST1OE:	
(09)	Project Code: **Timeshare**	
(10)	Logon At 11:20:10 PDT Tuesday 06/29/79	
(11)	CMS: R5.P02.Y29B 04/09/79 15:46	
(12)	** Notice ** CMS Field Test System	
(13)	R;	Data Security
	CMS	
(14)	C>ATT Pilist	
(15)	Enter Read Password:	
	Filist As B/A-Disk	
	R;	
(16)	C>LI * * A	Retrieval From File
(17)	ADDSDELS FOCEXEC B1	
	ALLABELS EXEC B1	
	ALLABELS FOCEXEC B1	
	BATCH1 EXEC B1	
	BATCH2 EXEC B1	
	CHANGES FOCEXEC B1	
	CLEAN EXEC B1	
	ET FOCEXEC B1	
(18)	??>KX	
	CMS	
(19)	C>T \ T\EDIT ADDSDELS FOCEXEC B	
(20)	E>T*	
(21)	TOP:	
	-START	
(22)	- Prompt &1.A1. Are There Any Additions To The Mailist Master File? Y or N.	
	-If &1 IS 'Y' GOTO ADD;	
	-If &1 IS 'N' GOTO NEXT;	
	Modify File Mailist	
	Prompt MC FT	
	Match MC	
	On Match Continue	
	On Nomatch Reject	
	Exit	
(23)	EOF:	
(24)	E>TOP	
(25)	TOP:	
(26)	E>L/PROMPT	
(27)	-PROMPT &1.A1. Are There Any Additions To The Mailist Master File? Y or N.	
(28)	E>C/Y/Yes	
(29)	-PROMPT &1.A1. Are There Anyes Additions To The Mailist Master File? Y or N.	
(30)	E>C/Yes/Y	
(31)	-PROMPT &1.A1. Are There Any Additions to the Mailist Master File? Y or N.	
(32)	E>C/Y Or N/Yes or No	
(33)	-PROMPT &1.A1. Are There any Additions to the Mailist Master File? Yes or No.	
(34)	E>FILE	Data Security
(35)	SET NEW FILEMODE AND RETRY	
(36)	E>QUIT	
(37)	R;	Log-Off
(38)	C>LOG	
(39)	CONNECT= 00:06:52 TRU=	
(40)	LOGOFF AT 11:27:02 PDT TUESDAY 06/19/79	
(41)	Please Log In:	

(12) The version of the operating system which the user is communicating with is a field test version--which means it is still being tested and has not been completely debugged yet. Field test versions are usually used only by in-house personnel at the time-sharing service.

Data Security (13-15 and 34-36)

The data security precautions in the system ensure that files belonging to a user are accessed only by those persons authorized to do so by the originator of the file. Passwords are the primary security safeguard.

(13) After the log-on and system messages, the computer indicates it is ready by typing "R;".

(14) The CMS system indicates it awaits a command from the user with the prompt "C>". In response to the CMS prompt, the user commands CMS to attach the disk with the storage space on it which corresponds to the user name "PILIST".

(15) Before the user can access the "PILIST" files, he must pass a data security check; he must know and type the "read" password which corresponds to the user name "PILIST". Generally, the read password is not the same password as the log-on password. The read password is given out by the originator of "PILIST" to persons he allows to read the contents of his files; the user may not modify the file in any way. In response to the CMS prompt, the user types the "READ PASSWORD" for "PILIST;" the password does not appear on the listing. An acknowledgement follows successful entry of the read password.

Retrieval from File (16-33)

In this series of interactions, the user retrieves data from a file and attempts to modify the data.

(16) The user entered the correct read password in (15). In response to CMS' ready signal and its prompt for a command, the user types "LI**A" that tells CMS to list the names and types of all files on disk "A", that correspond to the user name "PILIST". The code "B1" is a file security code that indicates a file has been established in a read and run mode and cannot be modified.

(17) The computer responds to the command in (16) by typing out a directory of files belonging to "PILIST". The listing is alphabetical. "ADDSDELS" is the name of one of PILIST's files; its file type is "FOCEXEC"--a language type; its security mode is "B1"that cannot be modified, but can be read if the correct read password is given by the user.

Log-On Authorization (03-05, 07-12)

In this series of interactions, the user must correctly identify himself to the computer system to be allowed access to data and computer resources. This step is the primary computer security defense against unauthorized users.

(03) The computer prompts the user for his user name, which may be from 1 to 8 digits. The user name serves to identify the storage space on primary disk, which belongs to the terminal user. However, before the user is automatically linked to the storage space corresponding to the user name he typed, he must verify that he is authorized to access the data stored there. The password serves as the verification key. After the user types in his user name (03), he must type the password that corresponds with the user name he typed. The user types his password on the same line as his user name; the password does not appear on the thermal paper on which this dialog appears.

(04) The user typed an incorrect password in (03), and the computer indicates this. The computer again prompts the user to type his password.

(05) The log-on security system is designed to prompt the user for his password repeatedly for 2 minutes following the user's first connection with the system (01). If the user fails to type in the correct password during the 2-minute interval, he is advised to contact his vendor representative, and his telecommunication link with the computer is automatically broken. This serves to deter unauthorized users from attempting to impersonate a user by guessing the user's password through trial and error.

Equipment Identification (06)

Failure to type the correct password in the 2-minute period necessitates initiation of the following procedure.

(06) The user must repeat the equipment identification steps (01 & 02) to reestablish a communication link with the computer. After establishing this link, he types in his user name and password as in (03).

Log-On Authorization (07-12)

After completion of step 06, the following procedure occurs.

(07) The computer's response indicates the user has typed in a correct password and is now in contact with the computer he wishes to use. The computer prompts the user to type in a project code, which is the session name that will appear on the user's bill. The system does not

check for a valid project code. However, the user is given a limited amount of time to type in either a project code or a carriage return, after which the computer will log him off the system. This is a security feature that deters unknowledgeable, unauthorized users. The user did not type a project code or carriage return within the time given, and the computer executed a log-off, at the time specified on the listing.

(08) In logging the user off the system, the computer did not break the user's communication link. However, to access the system, the user must once again go through the long-on authorization process, as in (03-04). The user responds to the computer prompt by typing his user name and his password; the password does not appear on the listing.

(09) The user has typed a correct password, and is prompted for his project code; he types "Timeshare," an arbitrary title.

(10) The computer responds by indicating that an authorized "LOG-ON" has been effected and gives the time and date of the log-on.

(11) The computer then identifies the operating system "CMS" with a code that details the version of CMS in use and when it was last modified; CMS is the abbreviation for "CONVERSATION MONITORING SYSTEM."

(18) The user stopped the computer from typing the entire directory of "PILIST" files by typing "KX"--the escape key combination. The user had probably already identified the file information he had been searching for.

(19) CMS prompts the user for another command. The user mistypes a "T" and erases it. This is indicated by the "T". The user then tells the computer he wishes to edit or modify the file "ADDSDELS FOCEXEC B".

(20) The computer responds by switching from the CMS language to a text editing language. This is indicated by prompt "E>"; the CMS language prompted the user by typing "C>", in line (14). The user commands the text editor to list all the contents of the file by typing "T*".

(21) The text editor complies and begins with the notation "TOF:", that means top of file.

(22) The text editor then lists the contents of the file as commanded.

(23) After the file has been listed in its entirety, the text editor system indicates this with the notation "EOF:"--end of file.

(24) The text editor prompts the user for another command. The user instructs the editor to go to the top of the file.

(25) The text editor indicates its "pointer" is at the top of the file.

(26) Prompted by the text editor, the user instructs it to locate and type the first sentence in the file with the word "PROMPT" in it.

(27) The text editor scans the sentences for the word prompt. It finds the word in sentence (22) and types out the sentence for user verification.

(28) The user responds to the text editor prompt by commanding it to change the first "Y" it finds in the sentence (22) to "Yes".

(29) The text editor follows the command precisely and prints the modified sentence for user verification; the first "Y" it located was in the word "ANY"; as per its instructions it substituted the "Y" for "YES" leaving "ANYES" in place of "ANY".

(30) In reviewing the modified sentence (29), the user realized that the word "ANY" had been modified instead of the letter "Y" at the end of the sentence as had been his intentions. He instructs the text editor to undo his previous modification.

(31) The text editor implements the user's instructions and types the modified sentence for user verification.

(32) The user responds to the text editor's prompt by instructing it to replace the phrase "Y OR N" with the phrase "YES OR NO", so as to avoid the problem he encountered in (28) and (29).

(33) The text editor implements this instruction and lists the modified sentence for user verification. The user notes that his intentions have been fulfilled; by switching the single character "Y" or "N", response choice to a multicharacter "YES" or "NO" response choice, he has modified the program in a way that will prevent it from running correctly.

Data Security (34-36)

The following steps are in response to the text editors request for another command.

(34) The user instructs the text editor to file onto disk the revised copy of "ADDSDELS" in place of the original.

(35) The text editor does not implement the user's command because "ADDSDELS" is a file of mode B; it can be read by persons who know the read password, but it can only be modified by the originator of the

file. The text editor instructs the user to modify the "FILEMODE" of "ADDSDELS" or to have the originator of the file modify it to allow the user to edit contents of the file.

(36) The text editor prompts the user for another command. Because the user is unable to insert the revised file into permanent disk storage, perhaps because his change was an unauthorized one, he instructs the editor that he wishes to cease his attempt at editing "ADDSDELS", and wants his revised copy deleted from the main storage of the CPU; the original file is left unchanged.

Log-Off (37-41)

In this series of interactions, the user completes his session, instructing the computer to "log him off", and basic accounting data are listed by the computer.

(37) The CMS system is now ready. The user is no longer communicating with the text editor.

(38) CMS requests a command. The user instructs it to log-off by typing "LOG".

(39) The computer types accounting details for the session just completed. "CONNECT" is the amount of time the user was in communication with the time-sharing service. "TRU" is the vendor's resource use algorithm, which combines I/O, CPU time, paging, and other services into one unit. Finally, the project code is listed.

(40) The computer notes that a log-off has been completed and gives the time and date it was effected.

(41) The computer awaits the next time-sharing session, requesting that the user sign-on.

Appendix G

REFERENCE TO LEGAL ACTION IN SELECTED CASES

Appendix G

REFERENCE TO LEGAL ACTION IN SELECTED CASES

The number of reported decisions in computer crime is minimal. To supplement the meager documentation, included here are references to some of those cases in the computer abuse file in which legal action took place. The listing is not represented as being complete either as to numbers of cases or to disposition of any given case. However, it is hoped that the references will provide a starting point for prosecutors confronted with similar fact patterns.

The numbers in the left margin identify the case. The first two digits correspond to the year of the perpetration. The third digit indicates the following:

(1) Destruction of property

(2) Intellectual property, deception or taking

(3) Financial, deception or taking

(4) Unauthorized use of services.

The last digit (or last 2 digits) is a sequence number indicating the order in which cases were discovered. [4]

FILE NO.	CASE DESCRIPTION
72222	A Santa Barbara insurance agent talked a Los Angeles resident into buying his insurance business by falsifying computer records to show $1,500,000 in annual business. The D.A.'s office did not understand computers, did not have hard evidence of falsification (records were deleted), and would have had to work through Santa Barbara; so they avoided the issue and got him on a noncomputer fraud issue. (Southern California)

72321

A food stamp clerk filled out and submitted a computer input form in her boyfriend's name. She was discovered only because her boyfriend's ex-girlfriend informed police about them.

Disposition: The clerk pleaded guilty to grand theft and presenting fraudulent claims.

73227

A real estate broker used a computer to comingle funds from good and bad investments. The D.A. avoided having to reconstruct the investments (to show misappropriation) by charging him with corporate securities violations. (Los Angeles, California)

7332

Stanley Goldblum, former chairman of the defunct Equity Funding Corporation, may be prepared to pay $100,000 in damages sought by former shareholders in a class-action suit. Goldblum, serving an 8-year term for his part in the fraud would pay the $100,000 over a 7-year period after his release. Payments would be made to Orion Capital Corp., the company formed after reorganization of Equity Funding. Goldblum was not included in the earlier settlement of the class-action matter. (U.S. District Court, Los Angeles, California)

7333

A programmer in a Monterey savings and loan embezzled money by illegally transferring money from 41 accounts into his wife's savings account through the use of the financial institution's computer. (California)

Disposition: The man was convicted and was sentenced to 1 year in prison.

7334

A California commodity options firm was sued by the California Dept. of Corporations seeking a court order barring the firm from selling commodity options on the grounds that such options should be regulated as securities. Lightning struck the computer room of the commodity firm so that some of its magnetic tape records were scrambled and thus on occasion million dollar errors appeared. (June 1973, California)

7336

The Sixth U.S. Court of Appeals in Ohio upheld a lower court ruling that Columbia Gas of Ohio must rely less on its computer in determining which customers were behind in payments and consequently should have their gas service terminated. The original class action suit alleged that customers had had their gas service terminated in violation of their constitutional right to due process. The problem arose when it was learned that because the company computer was located in another city, there was a time lag before payment information was fed into the computer. The computer was programmed so that whenever a bill was overdue, it issued a shutoff notice. This situation often resulted in shutoffs where customers had actually paid their bill or had made arrangements with the company to pay their bill.

Outcome: The company now has a manual system of review before any termination action takes place, and telephone access has been added to the computer equipment. (July 1973)

7337

An employee of Westinghouse was indicted by a New York Federal grand jury for embezzlement, conspiracy, and mail fraud. The embezzlement of $1,000,000 occurred when the designer of the computer auditing system manipulated that program to advise the master computer to issue forged corporation drafts. Six other men were indicted for conspiracy and mail fraud. (August 1973)

Disposition: The Westinghouse auditor and conspirators were convicted and sentenced to prison.

7338

File indicates two employees of a Southern California savings and loan embezzled $8,000 by creating 10 to 12 phony savings accounts by using a branch computer terminal. Loans were entered against each of the phony accounts and instructions for noncollection of the loans entered. The amount used to open each account was then withdrawn. (California)

Disposition: Employees fired and prosecuted. FBI report filed.

73314

A. Cowen & Co. brokerage house discovered embezzlement of $170,000 by a clerk in the firm. He was arrested, arraigned, held in lieu of $100,000 bail. Bail was subsequently reduced, and he was released on bail. There has been a presentation to the grand jury, but no indictment handed down. (New York)

B. Employee of Burke Sales Co., Seattle, Washington, pleaded guilty to embezzlement of $15,000 to $21,000 over 2 years. Released on personal recognizance and awaits sentencing. (Washington)

73326

Two employees of Consolidated Edison swindled the company for $25,000 by manipulating computer accounting records. They have pleaded guilty. (New York)

73327

Chicago Federal Grand Jury indicted 29 persons for criminal conspiracy in stealing $2.8 million from Steel City National Bank. (Illinois)

73328

SEC v. Fisco, Inc. (August 18, 1977) Charged with using a computer to understate losses and inflate profits to raise the value of stock. Civil action filed in U.S. District Court, Washington, D.C. The complaint alleged that all of Fisco's filings with the SEC, including the prospectus used in the second public offering, were materially false and misleading.

Disposition: Simultaneously with the filing of the complaint, each of the defendants, without admitting or denying the allegations, consented to the entry of judgment of permanent injunction enjoining them from violations of the antifraud and reporting provisions of the Securities Act of 1933 and the Securities Exchange Act of 1934.

In an administrative proceeding the SEC censured Kidder and Peabody (the underwriter of Fisco's second public offering) for negligence in attending to disclosure requirements.

7342

Theft and improper usage of a sign on/account identifier. (Wayne State University, Detroit, Michigan) (Letter April 23, 1973)

Disposition: Conviction obtained for obtaining services under false pretense.

7349

Colorado State Attorney General's office filed a suit against Computer Matching, Inc. in Denver District Court on behalf of two persons who claimed they were swindled by the computer dating service. The suit seeks a permanent injunction prohibiting the company from continued operation and recovery of fees paid by the two persons using the service. (Rocky Mountain News, October 17, 1973)

7414

Grand Jury in Santa Ana, California indicted the head of Dataspecs Computer Services, Inc. and his wife for conspiracy to commit arson and accessory to arson in connection with an explosion and fire at Computeristics, Inc. (The computer center was destroyed.) An employee of Dataspecs was also indicted for committing arson and burglary. (The Register, July 26, 1974, Orange County, California)

Disposition: Head of Dataspecs Computer and his wife were convicted of harboring, concealing, and aiding their employee with the knowledge that he had committed a crime. The head of the company was sentenced to 60 days in jail, fined $4,000, and placed on 3 years probation. His wife was fined $1,000 and placed on probation. The employee was convicted of burglary and arson and served a 2 to 20 year sentence at Soledad State Prison. (California)

7421

A state police officer and the president of a detective agency were found not guilty by reason of insufficient evidence of selling criminal records to supermarkets and department stores. This matter involved the police officer and the president of a detective agency allegedly removing criminal histories from computerized police files and selling them to stores for credit records and screening of prospective employees. This was the first case prosecuted under Massachusetts' privacy law. (Masschusetts)

Legal theory: The most significant piece of evidence at trial--a notebook containing the names of individuals whose records had been furnished to the stores found in the police officer's desk--was ruled inadmissible because it had not been furnished to the defense prior to trial.

Problems with case management: Attorney General office attorneys with no particular expertise in the privacy field were assigned to the case. Little importance was placed on the outcome. State prosecutors decided early in the case not to indict the detective agency itself, a case many attorneys felt would be easier to prove.

7425

Bechtel Corporation is suing Travel Service, Inc. in Alameda County to recover costs it says TSI owes in connection with a Bechtel computer installation. TSI has countersued for special and punitive damages alleging Bechtel failed to produce an operative system. Trial by jury to follow. (California)

7428

Computer programmer employed by Digital Equipment Corporation (Maynard, Massachusetts) stole system components valued at up to $750,000. He was arrested and charged with larceny of equipment, but released on his own recognizance. (Massachusetts)

7429

Manipulation of an automated inventory system at a wholesale distributing company resulted in theft of $20,000 worth of merchandise. Operation discovered by undercover drug agent buying drugs from thief. Men released by $5,000 bonds pending appearance in court. Arrested and charged with grand theft. (October 1974, Elgin, Illinois)

74219

England. A computerized security system for releasing containers at dockside in Liverpool was invaded through the use of false documentation. Falsified documents used to activate the release system enabled the theft of two containers. A four-person conspiracy was alleged, but failed legally.

Legal theory: Argument to the jury did not convince them of the reliability of the computer's documentation and logging system. A junior data processing clerk was insufficiently knowledgeable about the system and could not answer detailed questions about the program. A junior barrister was prosecuting the case.

Outcome. The stolen property was recovered in London and several men were sentenced to 2 years for handling stolen goods.

74222

Defendants used a computer to keep commodities records that allowed them to buy and sell quickly. This gave their firm the appearance of holding positions for clients, whereas they actually used a small amount of capital to finance a large volume of sales. The case was so complex and lacking of evidence that it was never prosecuted. But when the operators moved to Hong Kong and set up the same type of racket, they were caught.

Disposition: Five were indicted for grand theft, and four were convicted. No computer activity in the second operation. (Los Angeles, California)

7431

Airplane cleaner overpaid by computer, kept money and was charged with grand theft. (June 1974, San Francisco, California)

7437

Arrest of a supervisor of a/c receivable for an insurance company on embezzlement ($22,000). Charges employee put false vouchers through the computer, and the computer issued checks to bogus company. A clerk noticed unusually large amount of check. (May - July 1974, New York)

7438

Employee of unemployment compensation had input and monitoring responsibilities that she used to initiate payments. New employee ran audit and discovered payments. Suspended sentence, supervised parole for 5 years (first-time offender.) (Louisiana)

7439

S&L officer and D.P. Manager embezzled $4,000 from the institution's funds by modifying program to take advantage of a dormant a/c. Chose wrong dormant a/c and was caught the next day. Convicted in federal court. (September 1974, California)

74310

Drivers-licenses-for-sale-scheme included two DMV officials and two auto school owners. DMV examiner apprehended and charged with 46 counts of forgery, receiving bribes, and official misconduct. Face up to 42 years in prison if convicted. DMV cashier indicted on 11 counts of bribery. Auto school owners indicted on bribery, forgery, and related charges. (New York)

74311

Arraignment on credit card forgery in a department store credit card scheme. One suspect was an employee of the credit department. (November 1974, California)

74312

Japan. Man arrested on charge of stealing 2 million yen in cash from automatic cash dispensers by using counterfeit cards (December 1974).

74317

Holland. Employee responsible for preparation of suppliers' a/c substituted address information and had money credited to his personal a/c. Sentenced to 18 months "freedom" prison without probation and fined.

74321

England. Employee stole from savings department of bank by making false computer entries. Opened bogus accounts and reopened dormant accounts. Sentenced to 5 years in jail.

74324

Welfare fraud. Boyfriend of computer operator in welfare department plotted to remit false welfare checks with help of current welfare recipients who would kickback major portion of checks. He was sent to prison 1 to 3 years. Employee put on probation. (1975, Illinois)

74326

Man set up fictitious companies and procured bank loans for them by subverting large data bank. Pleaded guilty to federal fraud charges. Awaiting sentencing. (March 1976, U.S. District Court, New Jersey)

74327

The Harris gang planted members in legitimate businesses that subscribed to TRW Credit Data (Sears, etc.). The operation used and sold credit. Undercover agent arranged for purchase of credit credentials and caught Harris. Pleaded no contest to charges of making false financial statements, 2 years probation. (California)

74331

Norway. Conviction for gross fraud for stealing 1 million Norwegian Kr. Manipulated punched-card base for data processing entries. Continued over 4 years. Established imaginary firms and buyers with reference to installment contracts. Sentenced to prison for 2 years 6 months.

74332

Norway. Same woman as in case 74331 made false input into the EDP system on behalf of another firm which, as a result, had a large amount of business with the loan institution. She was sentenced for having manipulated the input of the contracts, accused of aggravated disloyalty, acquitted of the former in a new trial.

74339

Supervisor of a food stamp office inputted ineligible names and collected the stamps himself.

Disposition: He was caught and sentenced for grand theft and presenting fraudulent claims (also regarding an insurance firm he had worked for) and received 1 year in county jail, 14 months probation, and had to pay restitution ($18,000).

7511

France. Re: definition of property - tangible property. Accused person intentionally erased valuable information recorded on magnetic tape. Verdict of not guilty because tape itself was undamaged - no offense.

7522

West Germany. Nine persons arrested for disclosing secrets about Western electronic DP techniques (IBM technical information) to an East European secret service. Charges of theft, fraud, bribery, offenses against embargo rules and right of competition.

7524

Theft of heating oil--inventory discrepancies rigged in Exxon's (victim) computer. Oil diverted to another company. Indictment for receiving stolen property, larceny, and conspiracy. Two Exxon employees pleaded guilty to conspiracy. (New Jersey)

75210

Several employees of a furniture store were arrested for theft of merchandise valued at $200,000. The thefts occurred over an 18-month period by manipulating inventory data in the company's computer. (Pennsylvania)

75218

Bertram Seidlitz, a former employee of a national computer firm, was convicted of wire fraud in U.S. District Court in Baltimore, Maryland. The victim of fraud was Optimum Services, Inc., a computer service company under contract to several federal agencies to provide computer services. Defendant secretly managed to withdraw 18 of the 20 codes necessary to extract information from the computer program. It was the computer program itself that was valuable, not the information of the federal energy agency. This particular program (WYLBUR), developed at Stanford, gave OSI a competitive edge in its bid for government contracts. (U.S. District Court, Maryland)

Defense: Testified his theft of the program was an effort to show how lax the security system was.

Conviction: Two counts of wire fraud punishable by a fine of $1,000 or imprisonment of 5 years or both.

75219

The Select-A-Seat Corporation v. Bay Area Seating Services, Inc., et al. U.S. District Court Northern District of California C-750360 WTS. Second Amended Complaint filed February, 1976. The 2nd amended complaint asserts a claim against defendants for misappropriation of trade secrets and unfair competition by stealing and using the computer programs of the plaintiff to operate the Bay Area Seating Service. (California)

75221

Data Test Corporation v. Transamerica Computer Corporation. Transamerica by a contract signed in 1973 with Data Test was to supply computer equipment to be refurbished by Data Test. Data Test spent money to engineer and design computer refurbishing equipment. In 1974, Transamerica removed its equipment. Data Test sued Transamerica for $76.2 million for breach of contract. (California)

75244

Exxon Corporation filed a multimillion dollar suit against a former New Jersey state senator, his father, two of their family businesses and several other individuals alleging a conspiracy to defraud Exxon's Bayway Refinery of 16 million gallons of fuel oil over a 6-year period. The scheme involved pumping more fuel oil than authorized records showed and maintaining the deception through juggled computer records and rigged oil tank gauges. (New Jersey)

Defense: State senator and his father were innocents. The scheme was carried out between Exxon employees and defendants' firm without their knowledge. However, the state alleged they not only authorized others but also paid them to participate in the scheme.

Disposition: Former state senator and his father were found guilty of conspiracy and receiving stolen goods. They faced a possible prison term of 710 years and fines totaling $203,000.

7535

Man in Southern California pleaded guilty to receiving stolen property after he was involved in feeding false credit information into a computer credit verification system which allowed him to receive high credit ratings and thus purchase thousands of dollars of merchandise. (California)

7536

California Attorney General's office filed suit against a computer dating service for allegedly making false and misleading statements to enlist clients. The dating firm stated its program appealed mainly to professional persons, but they often matched persons with nothing in common. The suit seeks $2,500 for each misrepresentation, refunds to those subjected to unlawful practices, and a permanent injunction prohibiting unlawful practices. (California)

7538

A former Michigan welfare worker computer operator was convicted of 13 counts of mail fraud in a phony ADC check scheme that cost tax payers more than $25,000. The suit alleged the worker fed fraudulent information into the computer causing it to issue ADC checks to 15 of her friends. Maximum penalty for each count is 5 years in prison and a $5,000 fine. (U.S. District Court, Michigan)

7539

SEC filed a complaint against Standard Life & Accident Corp. alleging fraud. The FBI and U.S. Attorney's office in New Orleans and Oklahoma City have turned up evidence of twice-pledged collateral, computer fraud, executive self-dealing, forgeries, embezzlement and stock manipulation. (U.S. District Court, Oklahoma)

75310

London. A bank cashier was convicted of attempted fraud by trying to cash forged bank slips fed into the bank's computer. The slips were rejected by a new computer program, and the man was caught.

75312

A former payroll supervisor for Electrolux Corp. pleaded guilty to theft of $190,500 by manipulating the firm's computer. He was sentenced to 3 years of a 6-year term. (Georgia)

75329

A Los Angeles federal court convicted four men of conspiring to alter the personal credit ratings of individuals whose records were kept by the Credit Data Division of TRW, Inc. The defendants were accused of using a file clerk within TRW's facility to alter poor credit ratings by manipulating the computer entries for each individual. (U.S. District Court, Los Angeles, California)

Sentence: The ringleader received 60 days in jail to be served on consecutive week-ends, 5 years probation, and a $3,000 fine. The other defendants received 40 days in jail, 5 years probation, and a $1,000 fine.

75332

Insurance company theft. False medical claims were filed for operations never performed. Insurance company was to pay patient, not doctor. Patients received some of the money in return for cooperation. Indictments on charges of stealing by deceit or stealing without consent of the owner were handed down. Employee also involved. (Missouri)

75338

Mastermind of crime threatened two others involved. Scheme involved falsification of bank records and five check writing operations. Two bankers sentenced to prison for embezzlement. One got 2 years, another got 18 months. Third participant sentenced to 9 months. (U.S. District Court, Pittsburgh, Pennsylvania)

75339

Germany. Swindle in labor bureau in southern Germany. Employee of accounting department found flaw in system and exploited it. Filled out fictitious payment cards and fed them into computer which authorized payment. Went on for more than 1 year. Auditor discovered it by accident.

75343

Embezzlement by assistant claims supervisor and claims supervisor of a union health and welfare fund. Discovered by spot audit--second year in a row could not find same file; second time they looked for it and found evidence of wrongdoing. The missing account file showed that account holder cooperated with employee. Employee recommended to be charged with conspiracy and embezzlement. Other party to be charged with conspiracy and receiving stolen property. Husbands to be charged with receiving stolen goods. Women pleaded guilty to false pretense. (Maryland)

75344

Medical Fraud. Double billing after requests for payment were more than 1 year old. Consultant and claims supervisor cooperated in submission of false claims. Consultant pleaded guilty to presenting a false claim to a public board. (California)

75345

Accounts payable system fraud. Supervisor of accounts payable department entered false vendor code into computer, then entered false data regarding accounts payable to supervisor's sister. Original invoices and accounts payable distribution slips altered to show false vendor code. Information punched into computer, when there was a check run, sister was issued authentic checks. Indictment for transporting forged checks in interstate commerce dismissed--USC section states it does not apply to forged checks issued by company incorporated in foregin country (computer company were in Canada). Federal government appealing case. Brother pleaded guilty to deceit and defrauding and sentenced to 2 years in jail. (U.S. District Court, Maryland)

75351

A trucking firm employee juggled computer accounts and billings, pocketing the difference. It was discovered when he left the office, but he was not prosecuted because of the complexity of the case and because no witnesses were willing to testify.

7543

Police chief indicted for tampering with government records. Accused of having deleted reckless driving offense from his record in county's regional computer system. (Ohio)

7546

Man pleaded guilty to one count of grand theft for stealing $15,000 of computer time. He was placed on 3-month probation and ordered to make restitution. (California)

7547

A jury convicted a Newark, New Jersey man of advertising and selling phony computerized diets through the mails. Most of the diets were similar, but were supposed to be individualized by computer. (U.S. District Court, New Jersey)

Sentence: Could get 5 years in prison and $1,000 fine on each of 18 counts of mail fraud.

7611

An employee at the University of Maryland Hospital was charged with malicious vandalism when $100,000 damage was done to the hospital's computer. Wires and the master switch had been ripped out. Maximum penalty on conviction is a $500 fine and 1 year in jail. (Maryland)

76213

Three persons charged with fraud in connection with a credit information laundering scheme in Washington, D.C. Credit histories in computer data banks were altered to improve an individual's credit rating. All three pleaded guilty. (U.S. District Court, Washington, D.C.)

Sentence: Two were placed on probation and one sentenced to serve 6-18 months in jail.

76214

A Sears Roebuck former computer programmer and a police officer were arrested on charges of larceny by false pretenses when it was discovered that the former employee entered false paper work for approximately $10,000 of merchandise in the store's computer. The false paperwork bypassed the audit system. The charge carries a maximum 10-year prison term. (Michigan)

76219

A New York man was charged with mail fraud in U.S. District Court for devising a scheme to dupe purchasers of high-powered minicomputers. (U.S. District Court, New York)

Disposition: Pleaded guilty to two counts of mail fraud.

76220

F&M Schaefer Corp. filed suit against EDS for $115 million on charges that the software system EDS had been preparing under contract to Schaefer was faulty and had caused the beer manufacturer enormous damages. As a counter to the suit, EDS filed a motion asking repossession of the system or return of $1.3 million still owed on the contract. (U.S. District Court, New York City)

Arguments on the motion: Attorneys for EDS argued that the company had spent in excess of $4 million and several hundred thousand man-hours to develop the new program. They continued by noting that Schaefer executives had assured EDS that the turnover of the system was doing well. Schaefer claimed that the system EDS turned over to them in 1976 was the same system Schaefer itself developed prior to the contract.

Ruling: EDS's motion for repossession or repayment was granted on the basis that the EDS system was not the same as the original Schaefer system, and Schaefer did not have a performance clause in its contract, so performance was not a condition for payments or turnover of the system. The judge also found that the EDS software system was a tangible item and could be returned, despite Schaefer's argument to the contrary.

76222

Computer printouts were taken from the office of a government-sponsored program to obtain names, social security numbers and birthdates. These were used to write fraudulent IRS returns.

Disposition: One person from the program was among 14 indicted by a federal grand jury for conspiracy, filing false claims with the government, mail fraud, receipt of stolen property, and perjury. Most of these charges carry a maximum sentence of 5 years in jail and a $10,000 fine. Six ring leaders, not including the employee of the government program, were eventually convicted. Sentences varied from $10,000 and 6 years (for the "mastermind") to 2 years probation and psychiatric observation. (Southern California)

7631

A bank employee of 30 years pleaded guilty to federal grand jury charges of embezzlement. The employee juggled computer information to cover overdrafts and make illegal deposits to accounts of friends. She said she did it because the friends' business was in trouble and she believed they needed help. (U.S. District Court, Richland, Washington)

7635

Six men were indicted by a federal grand jury in Philadelphia on charges of embezzlement. A bank employee had access to a computer that showed dormant accounts, and with this information he devised a scheme to make fraudulent withdrawals from the bank's savings accounts. Loss estimated at $30,000. (U.S. District Court, Philadelphia, Pennsylvania)

7636

Woman indicted in embezzlement. A computer operator was to place bank deposits in correct accounts. Woman diverted money to her own account. (U.S. District Court, New Orleans, Louisiana)

7637

Indictment of two Blue Cross employees for scheme to process bogus claims through one employee's computer terminal. Thirty-one other persons charged with receiving and negotiating bogus claim checks. (New Jersey)

7638

Employees in Illinois Public Aid Department under investigation for tampering with computer so it would approve fraudulent, duplicate Medicaid bills. (Illinois)

76311

New Zealand. Payroll clerk pleaded guilty to feeding wrong information to computer and thereby stealing $1,176. Convicted and remanded on bail pending sentence.

76312

Damage suit filed against former department store bookkeeper. Was discharged when accused of embezzling. Fed wrong information to store computer; diverted checks made out to suppliers into two bank accounts in her own name and in name of fictitious business. Grand theft, forgery, possession of forged bills, and making or possessing fictitious instruments charges also. (California)

76314

Former computer systems employee at a bank charged with embezzlement and making false entries in the bank's records. Pleaded guilty to one count of false entry, given two years probation. (New York)

76315

Man arraigned on charge of interstate transportation of stolen property. Incident occurred when bank inadvertently credited $150,000 to a corporate savings account opened by the man. He removed the funds and converted them to his own use by transporting them to Oregon. (U.S. District Court, Eugene, Oregon)

76318

England. Health authority salaries officer stole 12,000 pounds from her employers. She handled payroll computer so doctors were paid both salary and expenses at end of month. Could pay expenses directly so she paid doctors by computer and had a hand-issued check made out which she put into her own account. Jailed for 12 months. Pleaded guilty to fraud charges.

76320

Norway. A man stole "cash card" forms (ready-made, printed and punched cards used to withdraw money from postal savings account) amount is entered manually. He had been a computer operator and programmer. He created an imaginary person and made cash cards which he presented for withdrawal. Clerks paid the money, but fraud was discovered when the cash cards got to the central EDP. Sentenced to 6 months prison - 21 days of which were unconditional while the remainder were conditional with 2 years probation.

76321

Welfare fraud. Three persons involved created food stamp accounts for five nonexistent persons. One of three was a computer terminal operator for food stamp office. Charged with fraud in obtaining public assistance. Sentenced to three years in prison. (Georgia)

76322

Four doctors and three medical groups accused of Medicare fraud conspiracy were cleared in Federal court. Fraud involved claims that medical tests were performed by hand in their offices when, in fact, tests were made less expensively by outside lab and Medicare billed at higher rate. (U.S. District Court, San Diego, California)

76323

Founder and former president of a security service pleaded guilty to embezzlement from the firm through a payroll padding scheme. Discovered by auditors. Submitted payroll information on fictitious employees as well as altering hours that real employees worked. He deposited false payroll checks to his bank account. (Washington, D.C. Superior Court)

7643

Computerized scheme to launder money gained in illegal activities. Used genuine commodity brokerage transactions as a cover. Front was business investment fund for doctors and other professionals in Texas. Illegal money funneled into the legitimate trust - by mingling with clean money, dirty money returned to Mafia front men posing as brokers. Busted by FBI undercover agents posing as potential "dirty money" clients. Tax attorney (mastermind) and sidekick expected to be indicted by jury. Possible charges are: conspiracy, making false statements, fraud by mail and telephone, interstate use of money obtained by racketeering. (Indictment expected from Federal Grand Jury, San Francisco, California)

7644

AITC (American International Trading Co.), a commodity trading firm, accused of widespread deceptive practices. Complaint filed by Commodity Futures Trading Commission - violated provisions of Commodity Exchange Act. Commission used computer list of firm's customers to ask them whether they had any complaints about AITC.

Possible sentences: The employee could get 180 years in prison and be fined $185,000. The accomplices could get from 15-45 years and be fined up to $130,000.

77110

Two California Department of Justice employees charged with deleting information from the criminal history system pleaded no contest to a related charge of malicious mischief. (California)

7721

A federal grand jury in Newark, New Jersey indicted the former president of Executive Securities Corp. for securities fraud and other offenses. The indictment charges that fictitious sales, alterations in computer and bookkeeping systems, fraudulent journal entries and concealment of records from the SEC were used to conceal Executive's failure to obtain physical possession of Centronic stock for McNeil customers. The grand jury returned 77 counts, including conspiracy, mail fraud, maintenance and submission of false business records.

7722

England. A British computer programmer who was fired from his job with the company stole the computer tapes containing all the company's financial planning data for the following five years. He attempted to ransom the company for approximately $470,000, as the information would have been highly valuable to competitors. The attempt was foiled and the man arrested.

7723

South Korea. An organized crime ring of South Koreans, with American help, exploited a U.S. Army computer to steal up to $17 million a year in American food, uniforms, vehicle parts, gasoline and other goods from Army installations in Korea in the early 1970's.

7725

A Santa Maria, California man charged with defrauding a local man and two businesses out of $18,000 by bogus advertising in nationally circulated computer magazines was convicted. Police had alleged that he advertised computer equipment he did not have, and that he filed false credit applications. (California)

Sentence: Two years and eight months in state prison for three counts of obtaining money under false pretenses.

7726

Two men in Miami were arrested for allegedly passing magnetic tapes, microfiche, and cruise missile components to Soviet agents and Eastern Bloc operatives. One man was already slated for trial in West Germany on charges of treason for passing material from West German DP firms to Soviet Bloc nations. (U.S. District Court, Miami, Florida)

7728

An agent for the Drug Enforcement Administration (DEA) was indicted for embezzling computer printouts from the Narcotics and Dangerous Drugs Information System for use in a scheme to identify DEA informants and facilitiate importation of marijuana. The drug agent and an accomplice entered pleas of not guilty. (U.S. District Court, New Haven, Connecticut)

7729

Oklahoma FBI agents attempted to find a man who had stolen sophisticated computer discs entrusted to his keeping. The federal complaint charged the Oklahoma City man with unlawful flight to avoid prosecution. The computer tapes were given to the man in an agreement that he would refine the programs they contained. It is suspected that he tried to sell them on the black market. (U.S. District Court, Oklahoma City, Oklahoma)

77213

A student at Queens College used the computer to tamper with his grades and those of a few other students, netting himself an unearned Phi Beta Kappa key. When a random audit picked up the discrepancy and the student (then working for the school) was informed, he resigned immediately. The school disciplinary committee is investigating but cannot revoke the student's degree if he had completed the requirements. Materials were turned over to the police, but no action has been taken against the student. (Flushing, New York)

77217

A man in Dayton, Ohio was convicted of three counts of complicity in tampering with credit records. He had upgraded credit ratings by manipulating computer information. (Ohio)

Sentence: Six months in jail.

77218

A grand jury in Illinois indicted a former police chief for selling criminal histories obtained from the state's computerized criminal information system. He pleaded not guilty. (Illinois)

77219

Three men were indicted for computer component theft of nearly $200,000. Two were to plead guilty to third-degree felony and one requested a trial. (Texas)

7731

A teller at a Washington, D.C. savings and loan office was charged with embezzlement by the U.S. District Attorney after illegally arranging the withdrawal of $18,000 from other persons' savings accounts. He used his computer terminal to locate savings accounts with limited activity, then transferred money from those accounts to fictitious accounts. Others were recruited to make withdrawals from the fictitious accounts. The teller pleaded guilty to embezzlement and his three friends pleaded guilty to false pretenses. An embezzlement conviction could result in a maximum prison sentence of 5 years, and a false pretenses conviction is a maximum prison sentence of 3 years. (Washington, D.C.)

7733

A former vice president of a New England bank was indicted for embezzlement and pleaded guilty. He embezzled $25,000 by manipulating the bank's computerized internal clearance account. (U.S. District Court, Boston, Massachusetts)

Sentence: Thirty days in Federal prison and performance of public service work 6 hours a week for 11 months without pay.

7737

Assistant Controller of First National Bank of Boston was charged by the U.S. District Attorney and pleaded guilty to embezzling $350,000 from the bank. The funds were embezzled on five separate occasions by transferring funds to the defendant's savings account. He covered the embezzlement by submitting through the computer false orders for cashiers' checks. He once submitted a duplicate bill for payment of services that State Street Bank had performed for First National. The defendant waived indictment and pleased guilty to a criminal "information." Could receive up to 5 years in prison. (U.S. District Court, Boston, Massachusetts)

7738

Eight people in Louisville, Kentucky were arrested by the FBI and charged with bank fraud, embezzlement, and conspiracy in withdrawing money from credit union accounts by manipulating computers. If convicted each could receive up to ten years in prison and a $5,000 fine. (U.S. District Court, Louisville, Kentucky)

7739

A former school board payroll supervisor (Fort Myers, Florida) was charged with grand larceny after he allegedly embezzled $109,000 of school funds. The computers had been manipulated to set up dummy accounts overcharging individual schools for teacher salaries and siphoning off that money. (Florida)

77311

A data processing specialist at a Texas savings and loan was charged with embezzlement of $450,000 by manipulating the computer to divert money from legitimate investment accounts to non-legitimate accounts. (U.S. District Court, Odessa, Texas)

77315

Three persons were arrested and charged with forgery in connection with the use of state computers to print fraudulent unemployment compensation checks. (Alabama)

Sentence:

1. One received 3 years in jail, to serve 6 months, and the remainder suspended on probation. Make restitution, sever all relationships with others involved.

2. Two received 3 year sentences, two months in jail, the remainder on probation. Make restitution and sever all relationships with others involved.

77318

A banker in North Carolina was accused of misusing $240,000 of bank funds through use of a computer. (U.S. District Court, Winston-Salem, North Carolina)

77322

Five men in Florida were arrested on charges of conspiracy and grand larceny for skimming money from the dog track betting system. The computer was rigged to boost the number of ticket winners in certain races and to print fraudulent winning tickets. Between $400,000 and $1 million was stolen in a 9-week period, and it may have gone on for 5 years. (Florida)

77324

Three persons were arrested on forgery charges for forging cancelled city payroll checks totalling $10,000. The checks were samples for computer testing purposes. (California)

77325

A San Francisco former bank operations officer was charged with embezzlement of $832,000. He pleaded guilty. (U.S. District Court, San Francisco, California)

Sentence: Five years in Federal prison.

77329

Two men bilked Union Planters National Bank of $3,885 by making false deposits and real withdrawals at the bank's ATMs. Deposited empty envelopes, withdrew at supermarket terminal. Indicted for conspiring to defraud the bank. (Tennessee)

77343

Computer fraud. False medical claims processed at Blue Cross. Checks made out to real and fictitious doctors, mailed to private homes, cashed by those involved in the scheme. Checks were for the cost of medical procedures never performed. (California)

77352

A clerk working for AT&T teletyped false overtime reports for herself to her company's main office and destroyed the replies. A random audit discovered the discrepancy. She would have been caught earlier if personnel had known the difference between the printed characters for zero and the letter O.

Disposition: She eventually pleaded guilty to grand theft and got 30 days in the county jail (suspended if $4,762 restitution was paid). (Los Angeles, California)

77354

A theater corporation owning 500-1,000 theaters employed vendors to service the theaters. An employee in accounts payable created a fictitious vendor, punched a computer card for it, and then submitted invoices for it. Also being responsible for mailing checks, he was able to pull the check before it was mailed and deposit it in a fictitious name business account. The suspect was caught when billing mistakes prompted a review.

Disposition: She was charged with four counts of grand theft ($23,000) and received 3 years probation and total restitution. (Los Angeles, California)

7741

Two former Sperry Univac employees convicted of mail fraud and conspiracy. Stole computer time. Computer programmers used computer to rearrange sheet music, then set up their own company to sell the arrangements. Not yet sentenced. (U.S. District Court, Eastern District of Pennsylvania)

7742

Mail order fraud. Letters sent out telling addressee that name was selected by computer. Letter promised vacation trip to Las Vegas for nominal charge. Criminal indictment for grand theft, false advertising, contempt of court. (California)

77412

Police officer wanted fancy tires. A thief told the officer about a car; the officer procured the owners' addresses. The thief then stole the tires. (New York City area, New York)

78209

A small computer was leased to the City University then "donated" for tax deduction. But it disappeared and a new one was leased. Appears to be theft, but no hard evidence. (New York City area, New York)

78210

A computer operator working for the police department was angry with his wife so he programmed the computer to report that her car had been stolen. She got picked up; he got fired. No prosecution.

78211

A recently terminated employee removed two tapes without signing them out. The firm suspected that he had copied or sold valuable information, but the Complaint Deputy refused filing for lack of evidence. (Los Angeles area, California)

78212

An employee dismissed from a small catalog sales firm retaliated by programming the computer to erase its files, resulting in $20,000 damage. Although there is circumstantial evidence (this employee was the only one with a key to log on), the firm does not think they will prosecute.

78213

An employee of an airline duplicated a computer application program he had helped develop. He formed his own company (while still working for the airline); used his employer's computer time, equipment, and employees to prepare the program; and sold two copies of it without paying royalties.

Legal issues: Defendant was indicted for grand theft. At the preliminary hearing, he argued that the program was not "property" but a "concept or idea" in his mind. Hence, he argued, the act was not theft but noncriminal duplication. Along the same lines, the judge was preoccupied with the question of whether there was any theft at all, because the airline still had the program. The judge determined that it was theft and set trial. The investigators determined that no copyright or trade secret violations could be found.

Disposition: The criginal damages were assessed at $15,000 (the price of the programs he sold) plus $900 (key punch time). These were later reduced to $30.00 for a disc and 1 cent per key punch card (which according to an investigator, would have been petty theft). Whatever the exact charges, defendant changed his plea to guilty at trial.

78314

An employee in a government agency broke a simple access code and learned how to issue a check to himself. But his girlfriend informed on him before he actually did it. Because he never actually committed a crime, he was never charged. (New York City area, New York)

78316

A clerk who put invoices on the computer invented a few fraudulent names. His friend was an accountant in charge of reconciling checks. They collected $217,000 over an 8-month period. Both were laid off pending investigation. (Los Angeles area.)

78317

A department store clerk used "returned merchandise" procedure on a computer to credit her own charge account. She was fired.

Disposition: Misdemeanor of $300 filed, but she was convicted only because she jumped bail. (Los Angeles area, California)

78318

A bank teller wired $150,000 from a large account to a well-known attorney's trust account. The unsuspecting attorney made the pickup and gave the money to other conspirators who are career criminals.

Disposition: The clerk was convicted of grand theft, not yet sentenced. The leader was not convicted because no one would testify against him. Three out of four of the others were convicted of grand theft. (Los Angeles area, California)

79202

A laid-off employee stole cassettes for a word processing machine. He attempted to extort his severance pay. Amount extorted was not relevant to conviction. (New York City, New York)

Disposition: He was convicted.

79203

An employee at ship-rating firm left the company and went to work for a competitor. It was found that several computer programs at the first firm had been suspiciously rerecorded, but nothing could be proved. The employer alleges it was stolen.

79204

A collection practice law firm had been a customer of a computer credit service and managed to use other user's identifying codes to avoid being billed for calls. (New York City area, New York)

Legal questions: Is the value of loss merely what the offending firm would have been charged? New York Theft Services Law (a misdemeanor) covers some things that are arguably not property. It would have been larceny if property were involved.

79205

A bank was closed by the State for unsafe banking practices. Computer records may have been tampered with. Unfortunately, FDIC (as receiver) sold some of the records. The case had not yet been tried, but DA thinks he can reconstruct the records to show unsafe practices. (New York City area, New York)

79206

A suspect company's computer records were seized, but the DA needed the company's help in choosing which records to demand and how to interpret them. The FBI took over the case from DA and is taking it before a federal grand jury. (Philadelphia, Pennsylvania)

79209

A security guard who was also a "computer nut" stole two computer terminals. Authorities suspect he was planning a large bank theft with an accomplice. Trial set for theft of equipment. (Los Angeles, California)

79210

Computer experts created a program for a lawyer. The experts were fired and later marketed a modified version of the same program. A lengthy investigation ensued.

Legal questions: Laws on patenting and trade secrets were not applicable; grand theft was the only charge that might allow the investigation to go further. But no one (lawyers, keypunch operators, other firms) knew enough about computer technology, and it got bogged down. There was no contractual agreement involved.

Disposition and factual issues: The case was finally dropped because: (1) there was never a complete program to compare with the attorney's; (2) no credible witnesses; (3) program may have been lawful ("knowledge in brain"); (4) company went out of business before any programs were sold; (5) lawyer still has the program, nothing was stolen. (Los Angeles, California)

79301

Employee filled out forms allowing the computer at his firm to write out checks to car companies. He then bought a car, returned it, got a refund, and pocketed the money. It was impossible to follow the paper trail, but suspect admitted his guilt after arrest and interrogation. Evidence included checks and forms. (New York City, New York)

79302

A customer service representative for a utility company falsified billing records in exchange for one-half the billing charges.

Disposition: Use of the computer resulted in anonymity hampering prosecution, but possible charges include: grand larceny, falsification of business records, forgery. (New York City area, New York)

79303

Union Pacific stock certificates were stolen by a computer officer. He knew the numbers to type on them to make them legitimate because he worked with the computer. He was caught only through a telltale I.D. mail envelope. (Eastern District, New York, New York)

REFERENCES

1. Donn B. Parker and J. Don Madden, "ADP Occupational Vulnerabilities," SRI International, Menlo Park, California (1978).

2. Donn B. Parker, Susan H. Nycum, and S. Oura, "Computer Abuse," SRI International, Menlo Park, California, Distributed by National Technical Information Service, U.S. Department of Commerce, Springfield, Virginia (1973).

3. Abraham Ribicoff, "Computer Abuse Control Bill," Press Release, January 25, 1979.

4. Donn B. Parker, "Computer Abuse Assessment and Control Study," Final Report, SRI International, Menlo Park, California (March 1979).

5. Brandt Allen, "Embezzler's Guide to the Computer," Harvard Business Review 53, July 1975.

6. U.S. Senate Committee on Government Operations, Problems Associated with Computer Technology in Federal Programs and Private Industry (U.S. Government Printing Office, Washington, D.C., June 1976).

7. U.S. Senate Committee on Government Operations, "Staff Study of Computer Security in Federal Programs," U.S. Government Printing Office, Washington, D.C. (1977).

8. U.S. Senate Subcommittee on Criminal Law and Procedures, "Hearing on the Federal Computer Systems Protection Act (S1766), June 21, 22, 1978," U.S. Government Printing Office, Washington, D.C. (1979).

9. Jay Becker, "Operational Guide to White-Collar Crime Enforcement, on the Investigation of Computer Crime," Battelles Law and Justice Center, Seattle, Washington (1978).

10. Howard Miller, "Manual for Prosecution of Computer-Related Crime," Atlanta, Georgia (1978).

11. Tim A. Schabeck, "Computer Crime Investigation Manual," Assets Protection, Madison, Wisconsin (1979).

12. John McNiel, The Consultant (Ballantine Books, New York, New York 1978).

13. Thomas J. Ryan, The Adolescence of P-1 (Collier Books, New York, New York, 1977).

14. Donn B. Parker, "Prosecutors's Experience with Computer-Related Crime," SRI International, Menlo Park, California (1979).

15. Donn B. Parker, Crime by Computer (Charles Scribner's Sons, New York, New York, 1976).

16. B.L. Lampson, "A Note on the Confinement Problem," Xerox Palo Alto Research Center, Palo Alto, California (1977).

17. U.S. National Bureau of Standards, "Federal Information Processing Data Encryption," Federal Register, pp.32395-414, August 1, 1975.

18. "Programming Language COBOL ANSI X3,23-1974," American National Standards Institute, 1430 Broadway, New York, New York (1974).

19. James Martin, Security Accuracy and Privacy in Computer Systems (Prentice Hall, New York, New York, 1976).

20. "Statement on Auditing Standards No. 3, The Effects of EDP on the Auditor's Study and Evaluation of Internal Control," American Society of Certified Public Accountants, New York, New York (1977).

21. "Codification of Auditing Standards and Procedures," American Society of Certified Public Accountants, New York, New York (1973).

22. "Standards for the Professional Practice of Internal Auditing," Institute of Internal Auditors, Altamonte Springs, Florida.

23. "Common Body of Knowledge for Internal Auditors," Institute of Internal Auditors, Altamonte Springs, Florida.

24. "Statement of Principle and Standards for Internal Auditing in the Banking Industry," Bank Administration Institute, Park Ridge, Illinois.

25. "Certification Program for EDP Auditors," EDP Auditors Foundation, 7016 Edgebrook Lane, Hanover Park, Illinois.

26. "Systems Auditability and Control Study (3 Volumes)," Institute of Internal Auditors, Altamonte Springs, Florida (1978).

27. Donn B. Parker, "Computer Abuse Perpetrators and Vulnerabilities of Computer Systems," Proceedings 1976 National Computer Conference (AFIPS Press, Arlington, Virginia, 1976).

28. Donald R. Cressey, Other People's Money, p. 147 (Wadsworth Publishing Co. Inc., Belmont, California, 1971).

29. U.S. National Bureau of Standards, "An Analysis of Computer Security Safeguards for Detecting and Preventing Intentional Computer Misuse," NBS Special Publication 500-25, U.S. Government Printing Office, Washington, D.C. (1978).

30. "Annals of the History of Computing," American Federation of Information Processing Societies, Arlington, Virginia (1979).

31. Leslie F. DeLashmutt, Jr., Captain USAF, "Steps Toward a Provably Secure Operating System," U.S. Department of Defense, Washington, D.C. (1979).

32. Richard A. DeMillo, Richard J. Lipton, and Alan J. Perlis, "Social Processes and Proofs of Theorems and Programs," Communications of the Association for Computing Machinery, Vol. 22, No. 5, pp. 271-280 (May 1979).

33. "Making It Count," Student Manual, Pamphlet 40701-003-1, Vol. 1, Boeing Computer Services, Inc., Seattle, Washington (1974).

INDEX

A

B

C

D

E

J

K

L

M

N

O

P

S

T

☆U.S. GOVERNMENT PRINTING OFFICE: 1979-311-379/1710

PRIVACY AND SECURITY DOCUMENTS

Other Publications of NCJISS Privacy and Security Staff

Privacy and Security of Criminal History Information: A Guide to Dissemination (NCJ 40000)

Privacy and Security of Criminal History Information: A Guide to Record and Review (NCJ 48125)

Privacy and Security of Criminal History Information: A Guide to Administrative Security (NCJ 49110)

Privacy and Security of Criminal History Information: A Guide to Audit (NCJ 59647)

Privacy and Security of Criminal History Information: A Compendium of State Statutes (NCJ 48981)

Privacy and Security of Criminal History Information: A Compendium of State Statutes 1979 Update (NCJ 59645)

Privacy and Security of Criminal History Information: An Analysis of Privacy Issues

Privacy and Security of Criminal History Information: An Analysis of Privacy Issues 1979 Update (NCJ 59646)

Privacy and Security of Criminal History Information: Users Manual (NCJ 59644)

Privacy and Security of Criminal History Information: Privacy and the Media (NCJ 59643)

Privacy and Security of Criminal History Information: A Summary of State Plans

Privacy and Security Planning Instructions (NCJ 34411)

Confidentiality of Research and Statistical Data (NCJ 47049)

Confidentiality of Research and Statistical Data: A Compendium of State Legislation (NCJ 44787)

END