D. B. Parker,[1] *M.A.*

Computer Related Crime

Computer crimes are acts resulting in losses, injuries, or damages that involve the use of information processing systems and come to the attention of law enforcement agencies. An information processing system includes at least one internally programmed digital computer as its chief component. The system may include input/output equipment such as punch-card readers, memory or storage devices, a communications network connecting other computers and devices, computer programs and data, materials, supplies, and human operators. Such systems are highly sophisticated, automated tools and repositories of information and data.

The physical nature of information processing systems and their functioning make them susceptible to penetration and use for antisocial activities. A system can be affected in four general ways:

(1) alteration of data and program input,
(2) alteration of processing and information output,
(3) alteration of a system physically through manual actions, and
(4) application of a system to antisocial purposes.

Known and suspected computer crimes as listed in Table 1 have involved the following actions which fit in the various categories above.

(1) Alteration of a computer program which changed the processing instructions.

(2) Theft of a copy of a computer program from a computer memory through telephone lines.

(3) Theft of computer programs stored near a computer in the form of punched card decks, reels of magnetic tapes, and printed sheets of paper.

(4) Theft of copies of computer processed name and address lists.

(5) Generation of input data to cause the output of unauthorized payroll checks.

(6) Use of a computer to measure the effects of manual alteration of company accounting records.

(7) Destruction of information processing equipment, materials, and supplies by fire, bombing, and striking with heavy tools.

(8) Destruction of magnetically stored data by magnetic field alteration.

(9) Erasure and loss of identification of data in a computer by unauthorized operation actions, including setting of switches and buttons and incorrect handling of punch cards,

Based on research performed on National Science Foundation Grant GI 30011 to Stanford Research Institute, for study on the Role of Criminalistics in the World of the Future.

Presented at the 25th Annual Meeting of the American Academy of Forensic Sciences, Las Vegas, Nev., 21 Feb. 1973. Received for publication 8 Feb. 1973; revised manuscript received 29 Aug. 1973; accepted for publication 13 Sept. 1973.

[1] Senior information processing analyst, Stanford Research Institute, Menlo Park, Calif.

reels of magnetic tape, magnetic disk-packs, continuous printer forms, punched paper tape, and operator instruction manuals.

Except for simple vandalism, all acts require a technical knowledge and skill obtained through extensive training programs and work experience with information processing systems. It is interesting to note that several prisons now offer data processing courses for qualified inmates [1]. In 1969 computer training was being offered to convicted felons in 26 states [2].

Twenty documented computer crimes occurring since 1966 are listed in Table 1. Three of them have been investigated in detail. Others are known only through trade publications, articles, and newspapers. The twenty cases break down as follows: seven cases of vandalism, four cases of larceny, eight cases of fraud, and nine cases of accident. There are many more computer crimes reported in newspapers and by rumor. Investigation of two supposed cases reported in the *Wall Street Journal* on 22 March 1971 showed them to be false reports of several cases conveyed by rumor, newspaper and magazine reports. They have never been verified and are suspected to be legends without basis in fact.

Information processing systems now facilitate the largest concentration of almost all of the sensitive and valuable data of business, government, and most other social institutions in the United States. Only the smallest of these entities are without information processing systems and services. Technical methods of protecting these systems exist to any degree desired, depending on economical feasibility. Several companies have been formed expressly to provide protective products and services.

Several casual conversations with key management people indicate that a large number of potential computer crimes are never brought to the attention of law enforcement agencies or made public. The reasons given are unfavorable publicity and ability to handle the situations privately. Crimes which first had been investigated by management were reported to law enforcement agencies for the following reasons: (1) the suspect refused to acknowledge his act, (2) management was unable to discover a suspect and feared repeated acts, or (3) reporting of the act, such as altered bank records, was required by law.

Until recently, possible computer crimes have been limited to financial and property loss (see Table 1 for details).

Financial Losses Estimated from Known Criminal Cases

$ 1 357	10/66
1 000 880	5/68
1 750 000	6/69
6 000	3/71
1 000 000	5/70
1 500 000	9/70
100 000	2/70
5 000	1/71
Average loss:	$ 670 400
Range:	$1 357–$1 750 000

None of the cases documented have resulted in injury or death. However, the potential for physical injury to humans is growing. Computers are now being used as part of life processes monitoring systems in medical surgery and intensive care of patients. Astronauts' lives are entrusted to computer systems for short periods of time. Air and street traffic are being controlled by computers. Computers are being used to control the landings of airliners. The scheduling of Bay Area Rapid Transit (BART) trains in San Francisco

TABLE 1—*Computer crimes.*

Case No.	Date	Reference	Verified	Type	Victim	Disposition	Description
1	10/17/66	*Minneapolis Tribune*, 10/18/66	Yes	Fraud Federal: Altering Bank Records	Bank in Minneapolis	Guilty plea, sentence suspended	Programmer altered his program to ignore overdrafts in his checking account of $1357
2	5/68	UPI, 1/15/69	Yes	Grand Theft and Forgery	Firm in Salinas, CA	Convicted, now serving 1–10 years in prison	Accountant embezzled $1,000,880 from 1963-1968—used a computer from financial modeling of his company to check that his thefts were small enough to avoid detection.
3	1968	Robert Bigalow	No	Grand Theft	Texas	Convicted, now serving 5 years in prison	Programmer took programs he wrote from his old employer to his new employer where he attempted to sell them
4	. . .	*Business Horizons*, 6/69	No	. . .	Anti-poverty agency in New York City	. . .	Data center employee printed unauthorized payroll checks of $1,750,000
5	3/29/69	*Computerworld*, 4/9/69, John E. Alman, Boston University	Yes	Vandalism	University in Boston	. . .	IBM 360/40 central processor damaged by wire cutting and acid
6	. . .	*San Francisco Chronicle*, 3/28/71	No	. . .	Firm in San Jose, CA	No charges	A bookkeeper embezzled $6000 through a computer system
7	11/12/69	*Computerworld*, 11/26/69	No	. . .	University in Massachusetts	. . .	Students gained control of computing center and threatened to keep it out of operation until demands were met by the administration
8	5/20/70	*San Francisco Chronicle*, 5/21/71, and *Computerworld*, 5/27/71	Yes	Arson Conspiracy	College in Fresno, CA	Indictment	A student led a riot in which a CDC 3300 was fire bombed—$1,000,000 damage
9	5/7/70	UPI, 5/8/70, and *New York Times*, 7/30/70	No	Conspiracy	University in New York	New York State Supreme Court restraining order, indictments	Students held the AEC computer for $100,000 ransom—incendiary devices were defused before damage was caused
10	4/70	*Computerworld*, 4/24/70	No	Fraud	People of the State of CA, Ass't.	Superior Court injunction, Judge R.	Computer dating bureau in Los Angeles charged with false claims

					Atty. General Andrea S. Ordin	Schauer, suit filed	that they were using computers to evaluate data and match clients
11	. . .	*Computerworld,* 9/2/70	No	Vandalism	University in Wisconsin	. . .	Data Center bombing, $1.5 million damage, 20 years of data lost
12	. . .	*Wall Street Journal,* 11/30/70	No	Accident?	Magazine publisher	Civil suit, $2.5 million	Programming and/or operator errors rendered subscription list useless
13	. . .	*Computerworld,* 12/23/70	No	Vandalism	University in Kansas	. . .	Data Center bombing—small damage to magnetic tape racks
14	5/28/70	*Computerworld,* 7/29/70	Yes	Fraud	Time-sharing computing service in Louisville, KY	Federal indictment violating Title 18, Section 1343	Customer made unauthorized use of a time-sharing service over a long distance circuit from Cincinnati to extract private data
15	. . .	*Computerworld,* 2/3/71	No	Embezzlement	Bank in New Jersey	Indictment	A V.P. of computer systems and a senior computer operator and three outside men charged with transferring money from infrequently used savings accounts to newly opened accounts—detected when conversion to a new computer disrupted work
16	9/24/70	*Computerworld,* 10/7/70	No	Theft, Conspiracy	Social services office in Los Angeles	Indictment by Grand Jury	Eleven employees used terminated state welfare numbers, changing names and addresses to issue checks
17	2/70	*Wall Street Journal,* 3/22/71	No	Vandalism	Chemical company in Michigan	. . .	Beaver 55 antiwar group destroyed magnetic tapes and punch cards—cost to reconstruct data $100,000
18	. . .	*Wall Street Journal,* 3/22/71	No	Larceny	Publisher	Civil suit, $4 million	Three million customer names list stolen by three night shift computer operators
19	. . .	*Computerworld,* 5/19/71	No	Larceny	Bank in Baton Rouge, LA	Federal civil suit, $5 million	Employee is claimed to have taken programs he wrote for his bank to his new employer, a bank in Garden City, Kansas
20	1/19/71	*Oakland Tribune,* 3/2/71	Yes	Grand Theft	Service bureau in Oakland, CA	Indictment civil suit, $6 million	Programmer accused of stealing a copy of a computer program from his employer's competitor over phone circuits from a remote terminal in Palo Alto, CA

will be done within close tolerances by computer. These systems have fail-safe features and are closely monitored by humans, but in some emergencies it will be thought safer to take a chance with the computer than to trust control to humans.

Information processing systems already are indispensable to the functioning of society. The U.S. Social Security Agency now uses 13 IBM 360/65 computers. The entire system, with millions of people paying into their retirement funds or receiving their benefits, would stop without those computers. Insurance premium notices, magazine subscriptions, and tax bills could not be processed even with the entire work force of the nation replacing the computers. The defense system of the United States would be helpless. The next step will make computers indispensable to each other, as nationwide networks are formed to electronically communicate between them, thus reducing the need for intermediate production of information in hard form on paper or recorded on magnetic tape for transportation between computers. This will reduce the possibility of tampering with the information in present-day unsophisticated ways, but each advance will create new, more technically complicated ways of performing computer crimes. This presents a challenge to law enforcement agencies. They must also grow rapidly in technical sophistication.

Incidence of known computer crimes to date is small—twenty reported crimes since 1966. Informed guesses are that 85 percent of all crimes are unreported [*3*]. This would result in an incidence of both reported and unreported crimes at over 130, or about 26 per year, in the United States during the last five years.

The impact of information processing systems and future incidence potential can be roughly measured by the size of the information processing business and its expected growth over the next five years. Sources at Stanford Research Institute (SRI) indicate that there are 80,000 computers currently in use in information processing systems. Annual sales of computers are at the seven-billion dollar level. By 1975 this should reach 140,000 computers at an annual sales level of 14 billion dollars. By 1980, annual sales should reach 18 billion dollars and represent 14 percent of all equipment and machinery manufactured in the United States.

In addition to this market a new product, the minicomputer, will have a significant impact on business. Minicomputers are miniature computers selling for less than $55,000. Sixty percent of them will find use in small businesses with annual sales in the range of $500,000 to $10 million. According to the IRS statistics of income there were 267,000 such businesses in 1970 and there will be 311,000 in 1975. This market is very large. SRI sources indicate there were 3000 minicomputers used in business applications in 1970; there are expected to be 43,500 by 1975. Minicomputers represent an important factor in computer crime. They tend to be operated in less formally controlled environments by relatively untrained people, yet they will be used to process data of equal value to large computers, relative to criminal motives.

For example, a minicomputer will be commonly found in large auto dealerships where there is normally only one accountant with an assistant and a newly hired computer programmer also serving as an operator. The typical programmer/operator will have a high school education and a ten-week programming course. Yet the management and accountants must rely completely on this young person for all financial data processing for the firm on its new $50,000 minicomputer, which does not have an audit feature understandable to a non-computer-oriented individual.

Most of the remaining 40 percent of minicomputers are in non-business applications in industry, transportation, education, and government. These minicomputers will also be vulnerable to criminal intentions and more likely to result in physical harm to people.

The growth in numbers of trained people engaged in development and operation of information processing systems is equally impressive. The following statistics are from SRI sources:

Computer Personnel	1970	1975
Systems analysts and programmers	500 000	900 000
Computer operators	200 000	450 000
Keypunch and data preparation aides	580 000	880 000
Total	1 280 000	2 230 000

By 1975 this will represent about three percent of the 80 million people work force in the United States.

The criminal use of computers is not limited to those people directly involved in developing and operating the systems. Vandalism and fraud can be perpetrated by other people taking advantage of otherwise legally operated computers. The number of people directly involved in the operation of each computer was 14 in 1970 and will decline to 10 in 1975. For rough approximations, it is assumed that an equal number fall into the category of people who can also engage in computer crime. This puts the total number of people at two and a half million in 1970 and four and a half million by 1975, representing six percent of the labor force.

We can now apply general crime incidence factors to the above estimates to produce first-order guesses at computer crime incidence. Unfortunately, computer crimes fall into the category of white-collar crimes, about which little is known.

The FBI 1970 Uniform Crime Report indicates that 4354 property crimes per 100,000 population were reported in 1970 in cities over 250,000 in population. Assuming that most computers are located in the larger urban areas and applying general property crime statistics to people in contact with information processing systems, the annual incidence of general property crime in 1970 was 0.0435 × 2,500,000 = 108,750. 8.8 percent of convicted felons in 1965 in Washington, D.C., were clerical/sales people and managers, as concluded by SRI in the 1966 President's Commission on Crime in the District of Columbia. Applying a figure of ten percent we might conclude that the annual incidence of general property crimes among clerical/sales and managerial people is about 10,000 for all large urban areas in the U.S.A. This obviously is a soft figure, and it would be of little use to apply in our case. This is especially true since the figure refers to FBI crime categories which do not include fraud, embezzlement, conspiracy, vandalism, or extortion.

These figures also do not take into account that the number of crimes are not in a one-to-one proportion to the number of criminals. In fact, computer crimes tend to consist of multiple crimes per incident. From the criminal cases studied (see Table 1) the programmer in Minneapolis (Case 1) was convicted of two counts of altering bank records. Actually, the records were altered every day for four months. The accountant in Salinas (Case 2) was convicted for both grand theft and forgery. He perpetrated his crimes over and over for six years. A different concept of what constitutes a single criminal act will be necessary, considering that computers can be programmed to perform illegal acts up to several million times per second and even cause other programs to be altered, which in turn can result in further incidences in the same or other computers.

The financial benefits to perpetrators of computer crimes is almost unlimited when one considers that primary records of almost all of the wealth of the United States pass through information processing systems. This includes corporate revenues and expenses, banking, securities, social welfare, U.S. foreign aid and Department of Defense moneys, social security, and taxes. This might be tempered by known computer crimes where one of the largest amounts of money taken was one million dollars. However, in this case the criminal was successful for seven years before he was caught. The repetitious and unchanging nature of computer functioning implies that once an alteration of an informtion processing system has been made, a continuing flow of illegal activities can occur.

The President's Commission on Law Enforcement and Administration of Justice Report of 1967 estimates the following losses from crime:

Crime	$ Loss in Millions
Embezzlement	200
Fraud	1350
Tax Fraud	100
Forgery	80

Not only must these figures be questioned, but some method would have to be devised to deduce what fraction involved the use of a computer or computer related materials. A survey of business and government information processing systems managers would be most fruitful in determining incidence and potential for computer crimes.

Incidence will also be affected in some as yet unknown way by the preventive measures currently being promoted and popularized among information processing systems management. In particular, large banks have become sensitive to computer security. The American Management Association, Advanced Management Research (AMR International, Inc.) and others frequently offer management seminars on the subject. However, it is expected that the increasing number of systems (55 percent annual increase in the minicomputer market by SRI estimates), and the increasing reliance on them in the functioning of society, will make the opportunities for criminal acts outweigh their suppression by increased security measures.

Society is starting to develop an awareness of the extent to which computer technology is affecting and becoming an integral part of the functioning of society. This is evident in the public media, congressional hearings, and consumer advocacy efforts. Business and government are increasingly putting their trust in information processing systems, for systems are becoming more complex than any one person (even a systems expert) can understand. During 1971, the First National City Bank of New York City spent $900,000 on computer system validation and auditing alone.

Consumers had far more problems with manual systems before automation, but the often illogical nature of information system failures is foreign and thus illogical to the layman. This disquieting image of "giant electronic brains" serving and affecting the public makes computer crimes quite sensational and blown up beyond reasonable perspective.

One computer crime case (Case 20) illustrates this situation. In 1971 the alleged theft of a computer program from Information System Design (ISD) in Oakland, Calif., worth $5000 received great public attention. It appeared in all major newspapers in the United States. It resulted in three-inch, front-page headlines in the European editions of the *Herald Tribune*. It occupied the front page of the *Oakland Tribune* for several days and produced headlines in all of the San Francisco Bay area newspapers. Compare this to the meager publicity of the thousands of $5000 auto thefts. Thus, the value to business to suppress news of computer crimes is very high. This factor is important in estimates of incidence.

The actual levels of financial loss are not nearly as important as the incidence, number of victims, and extent of disruption of personal business and commerce. The exposure of private information stored in information processing systems to unauthorized people is considered at least as serious as financial loss. It is suggested that quantitative values to society of the prevention, detection, and solution of computer crimes might be extrapolated from the quantitative values placed on non-computer-related crimes of similar nature. More importance might be placed on the following crimes when a computer is involved: extortion, blackmail, larceny, fraud, embezzlement, forgery, vandalism, and grand theft.

Law enforcement agencies will increasingly encounter computer crimes and the evidence associated with them. This represents a new technology for the crime laboratories and investigation officers. Fortunately, computer technology is starting to be used by these same agencies for their internal information processing. Thus, persons with the technical expertise already exist within the larger agencies. A program of making this expertise known and effectively using it should be instituted.

The most difficult type of evidence to deal with is information stored in magnetic and electronic form. It is not directly readable by humans. Copies of it can be made, and it can be altered, used for devious purposes, and restored, all in only one thousandth of a second. It can be sent across the country through telephone circuits without any records of the event. Protective methods and recording of events must also involve the magnetic and electronic storage of information. The layman can only trust the computer technologist that information he receives in human readable form accurately represents the stored information in the computer. There is no authoritative source describing the basic principles of computer technology. The technology has changed too fast. However, there is a growing demand for such documentation. Computer programming has been strictly an art. Only recently have there been efforts started to transform it into a science and field of engineering and business. A programmer's work is almost impossible for another person to check in detail. There is no computer program of any substance in existence today which can be guaranteed free from all logical errors. The most esoteric aspects of computer science are just starting to find methods of proving the mathematical correctness of simple computer programs.

Law enforcement agencies are facing computer crime problems today as evidenced by the following search warrant and related facts in a case of theft of trade secrets, handled by the Oakland Police Department and District Attorney's Office.

Example: Search Warrant issued by Municipal Court for San Jose-Milpitas Judicial District, County of Santa Clara, State of California. Requested by Terence Green, Fraud Detail, Oakland Police. Theft of trade secrets 499c California penal code to search UCC, Inc., H. J. Ward residences, auto, and person. February 19, 1971.

Property specified:

(1) Keypunch computer cards punched with ISD remote plotting programs.

(2) Computer printout sheets with printouts of ISD remote plotting programs.

(3) Computer memory bank or other data storage devices magnetically imprinted with ISD remote plotting computer programs.

Inventory of items taken:

(1) Listing of names of files on Fastrand drums.

(2) Abbreviated file directory description listing of Fastrand files as of 0730, 2/19.

(3) Abbreviated description directory of files "dumped" from Fastrand at 2300, 2/19/71.

(4) Nine tapes as result of "dumping" item (3).

(5) List of 19 tapes assigned by UCC to H. J. Ward.

(6) Program listing of a computer run, 2/2, 12:05:08, sequence no. 180.

(7) Nineteen tapes in plastic containers listed in item (5) above.

(8) Binder of listings of computer runs labelled "Aerojet-General J. Ward."

(9) Disk file folder containing:

(a) handwritten ISD message format description.

(b) ISD UNIVAC Users Guide manuals.

(10) Manila folder labelled "Plot Packages" containing CALCOMP plotter manuals.

(11) (Not taken.)

(12) Manila folder labelled "Aerojet-General" containing handwritten and printed pages.

(13) Manila folder labelled "Aerojet-CALCOMP" containing five xeroxed pages labelled ISD, printed and handwritten pages.

(14) Binder labelled ISD containing a number of listings of computer runs.

Sergeant Green was questioned as a witness on 7 Sept. 1971 at the preliminary criminal hearing for H. J. Ward before Oakland Municipal Court Judge W. F. Levins. He testified that the search was carried out by himself, Keith Marcelius, Don Ingram of the Oakland District Attorney's Office, and a Palo Alto policeman. They searched the computer room and H. J. Ward's office. Marcelius identified items to seize. The UCC attorney was present. The UCC staff carried out the Fastrand dumping and gathering of tapes under direction of Ingram. Under cross-examination, Green stated that Marcelius specified the items in the search warrant and identified and specified all items to be seized. Green also stated that he had no knowledge or understanding of any of the materials and could not have recognized such materials at the time. The following items supplied by ISD and others seized in the search were accepted as evidence in the hearing:

(1) Keypunch card deck of 515 cards containing source program, PLOT/TRAN.

(2) ISD UNIVAC 1108 console log covering a portion of time on 19 Jan. 1971.

(3) ISD monthly billing records of 19 Jan. 1971 for Shell Development Corp.

(4) ISD program listing of PLOT/TRAN.

(5) Listing of a program taken from H. J. Ward's office.

(6) Picture of a UNIVAC 1108 computer.

(7) Hand-drawn chart describing the ISD computer and remote terminal configuration.

(8) Report by the expert witness of his comparisons of the ISD materials and materials seized at UCC.

The expert witness, Dr. Ned Chapin, examined the evidence and testified that the punch card deck and ISD and UCC listings all contained identical parts of computer programs. Ward pleaded guilty to theft of a trade secret and received a suspended sentence and was fined.

This case is an example of the types of problems law enforcement agencies face with advancing computer technology.

In summary, advancing computer technology and its use for sensitive functions in society are fast outstripping a capability to protect assets being processed in computers. The fields of jurisprudence and law enforcement are not yet prepared to contend with the abuse of this new technology. However, the use of computers in criminal acts is just beginning, and there is an opportunity to take the offensive if we act now through research, education, and legislation.

References

[1] "Oregon Penitentiary," *Computerworld*, 27 April 1970.

[2] Bemer, R. W., Ed., *Computers and Crisis*, Associations for Computing Machinery, New York, 1971, p. 12.

[3] Hood, R. and Sparks, R., *Key Issues in Criminology*, World University Library, 1970.

Stanford Research Institute
Menlo Park, Calif. 94025