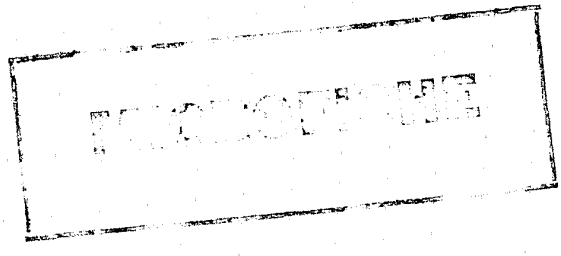
TEXAS

CRIME PREVENTION INSTITUTE

Specialized Data School For Crime Prevention Officers



SOUTHWEST TEXAS STATE UNIVERSITY

SAN MARCOS, TEXAS

In Cooperation With

CRIMINAL JUSTICE DIVISION

OFFICE OF THE GOVERNOR

STATE OF TEXAS

SPECIALIZED DATA SCHOOL

FOR CRIME PREVENTION OFFICERS

Prepared for

SOUTHWEST TEXAS STATE UNIVERSITY

TEXAS CRIME PREVENTION INSTITUTE

by

Dr. James Poirot
Mathematics Department
Southwest Texas State University
San Marcos, Texas

Bronwynn Berish
Crime Prevention Analyst
Garland Police Department
Garland, Texas

Geraldine Caldwell
Intelligence Analyst
Dallas Police Department
Dallas, Texas

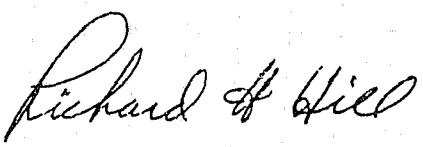
Peter A. Stone
Records Management Consultant
Texas Commission of Law Enforcement Standards and Education
Austin, Texas

ACKNOWLEDGEMENTS

The development of the Specialized Data School for the Texas Crime Prevention Institute could not have been undertaken without the aid and assistance of many people.

First we would like to acknowledge the individuals who spent untold hours developing the material for this text: Dr. James Poirot, Mathematics Department, Southwest Texas State University, who coordinated the efforts of all participants and provided substanial input in all materials used; Ms. Bronwynn Berish, Crime Prevention Analyst, Garland Police Department, who developed new material and whose experience and input in the area of crime prevention analysis was invaluable; Ms. Geraldine Caldwell, Intelligence Analyst, Dallas Police Department, without whose assistance this text would not have been complete; and Peter A. Stone, Records Management Consultant, Texas Commission on Law Enforcement Standards and Education, Austin, Texas, who provided input in the area of records management.

The Texas Crime Prevention Institute wishes to express its appreciation to Mr. Bob Goss, Director of the Computer Center, Southwest Texas State University, and Mr. Richard Beaver for their assistance in programming and for scheduling the computer center for the use of the Texas Crime Prevention Institute.



Richard H. Hill, Director
Texas Crime Prevention Institute
Southwest Texas State University

TABLE OF CONTENTS

IMPLEMENTING A NEW CONCEPT IN A TRADITIONAL SYSTEM

Whether the crime prevention analysis function be accomplished by a civilian analyst, a law enforcement officer, or a person responsible for crime analysis on a regional basis, the individual(s) are faced with not only implementing a relatively new concept within a traditional environment, but with functioning within both a formal and informal structure. The multiple facets of the public with whom the analyst must deal, depending on his particular job description, may include city managers, chiefs, sworn officers, ranking officers, citizenry, and other individuals of like responsibility as his own. The analyst must be aware of the potential help and support he may receive and likewise give to his constituency.

In many areas the position of crime prevention analyst has either never existed before or is relatively new. Conversely the law enforcement agency itself has existed in basically the same form for several decades. Bearing this in mind, an analyst entering an agency must realize that he will be dealing with people having years of experience in understanding and dealing with crime trends, analysis of these trends, and techniques for the prevention of crime although this sometimes only "gut feeling" may or may not have ever been formalized. The analyst can therefore draw a wealth of information from the constituency he is serving.

"Red flags" should go up in the minds of any analyst (because they will in the minds of his peers) that approaches the subject of crime analysis with the attitude that through crime analysis he alone can solve the crime problem. Think twice before making a statement like the

following: "If you do such and such, I guarantee your problems will be solved".

An analyst is not a soothsayer and cannot say that by subtracting B from A you unequivocally will get C when dealing with crime data. The analyst can by studing the data, by considering as many variables as possible, and by drawing on the experience of others, present the facts gleaned from the data and suggest realistic possibilities to be considered for solution.

Communication

As suggested before, communication must be open in order to receive the information needed for analysis and also to present the information prepared by the analyst. A helpful hint to remember is that communication, whether formal or informal, will necessarily be structured differently dependent upon the makeup for the group with whom you are communicating.

For instance, if you are talking to a more advanced group, you may want to discuss in terms of "detailed statistical analysis" mentioning the different types of statistical methods you used in your evaluation. However, if you wanted to present the same information to a group composed of persons functioning primarily in the area of enforcement the more sophisticated approach using statistical terminology may result in a "turn-off". Don't talk down to anyone, but do not try to talk over their heads either.

When communication is kept open, the analyst stands to gain as much help from his peer group as he provides them.

Understanding the Organizational Structure

Before the analyst can affect a functional analysis unit and before there can be successful communication within the total organization, he must understand the Organizational Structure of the agency with whom he will be working.

The first step towards accomplishing this may necessarily be to sit down with a copy of a formal organizational chart of the agency to determine the structural hierarchy. Because of the structural likeliness to a military organization existent within law enforcement agencies, an understanding of the chain of command is important to an analyst's success. A sworn officer functioning in this position won't have the difficulty in recognizing the chain of command that a civilian or possibly regional planner may have. The analyst, new to the law enforcement environment, will find that by understanding the organizational structure, he will know where he can find the data he wants for his informational needs and, who to approach to get this data. In a law enforcement agency, the shortest distance between two points is not necessarily a straight line.

Once the crime prevention analyst is established, and gains some insight into the people around him, he may find the existence of a more informal organizational structure. In this type environment, the analyst can often times accomplish a perceived goal in a more informal way, (i.e.

oral communication through informal talks) by communicating directly with the individual most familiar with the information the analyst needs. He may also find that in the informal organization a wealth of information may become available to him that would be virtually unobtainable from strict compliance to a formal organizational structure. The analyst will with time and insight learn to discern the most reliable information sources.

Helpful hints:

1) Know the people you worth with.

2) Allow them to know you.

3) Be thorough in your evaluation of any given problem.

4) Be open to suggestions from peers on all levels. (i.e. listen)

5) Be able to substantiate any conclusions you draw.

Suggested Readings

Managerial Psychology - Harold J. Leairtt

Organization for the Public Service - John D. Millett

Games People Play - Eric Berne

OBJECTIVES IN CRIME ANALYSIS -

WHAT, HOW, WHY?

What. An objective is a problem to be solved, a statement of What you want to do. Usually it is written and fits within the overall Goals or Objectives of the Department. Too often it was merely a gentleman's agreement among staff. Today, however, cities are productivity and cost oriented, causing police agencies to more closely monitor their operations.

A departmental statement of objectives allows for easier evaluation of Operations and Support Services for use by Administration. Objectives specifically for crime analysis should state What is to be accomplished, and allow for How and Why. Since most departments have not dealt with analysis of crime, objectives may be overly vague on one hand, and overly confining on the other. Compounding a lack of understanding of Analysis, along with many different Crime Prevention definitions and approaches further confuses the setting of objectives.

With the above statements in mind, objectives for Crime Prevention Analysis should follow certain universal guides:

I. Answer unique community requirements.

   A. Fit within definition of major crime problems (or define what they are).

   B. Fit within existing departmental objectives.

II. Allow for statistical measurement (for cost and evaluation).

A. Use key words that are presently statistically oriented.

1. Offenses
2. Arrests
3. Cases
4. Clearances
5. Reports
6. Time (hour, day, month)

B. Allow statement to define cost and personnel needs generally.

III. Use some experimental objectives where the objective is "to determine" or "to define" future projects or data needs or cost figures.

IV. For funded projects, time frames must be allowed for (monthly progress reports or meetings, charts).

How. Now that an objective has been defined as a What, the next question or problem is How. For the purposes of Analysis, this will deal with statistical methods to be used for:

1. Administrative decision making.
2. Determining priorities for operational units.
3. Defining evaluative standards.
4. Determining information or data needs.

Once objectives or problems are committed to, Analysis, as a support function should be cautious to follow objectives closely. When setting up implementation or How, be certain, as a new concept, to stay within the bounds of each problem; Administrative or Operational.

The crux of Analysis is set out in two statements:

1. What the Chief of Police would do, if he had time.
2. Converting raw data into useable information.

As was mentioned previously, make use of charts, and meetings. Monthly or quarterly reports need to be discussed and/or graphed so all levels can see and discuss the progress of the objectives, and How each area is functioning.

Analysis depends on sources outside itself for collection and quality of data, and must work within a pre-established system, that is not necessarily oriented toward analyzation. Changes may need to be made, however. Analysis within new units cannot always be reduced to an exact science. Use inductive logic in approaching problems and How to solve them.

Why. Justification, evaluation, and accountability are judged on many different levels.

1. Necessity (priority)
2. Manpower (operation and support-clerical)
3. Equipment and space
4. Cost includes all of above

If objectives (What the problem to be solved is) are stated clearly at all levels of the department, and accurate records of How problems are being solved or objectives met are being maintained, then Analysis will be able to account, in terms of cost and productivity, for the necessity of continuing or discontinuing stated objectives.

Review of Objectives

What - Chief of Police needs to meet community demands and problems, stated clearly within existing departmental objectives.

How - Convert raw data into useable information (administratively and operationally).

Why - Justification of methods to accomplish problem solution.

For reference see: Prescriptive Package, Police Crime Analysis Unit Handbook, U.S. Department of Justice, L.E.A.A., National Institute of Law Enforcement and Criminal Justice. Chapter II, A. Definitions of Goals and Objectives, Pg 7, and Automated Police Information Systems, Paul M. Whisenand and Tugt. Tamaru, John Wiley and Sons, Inc., New York, 1970. Chapter 4.

LAW ENFORCEMENT RECORDS

ANALYSIS AND MANAGEMENT

> Management of a police department is similar in many respects to management of any of the larger business enterprises in the community. There is one significant difference, however. The police "business" is one that directly involves the liberty and safety of every person served by the police organization.[1]

Information is what allows any law enforcement agency to function. However, each agency must evaluate its own needs and how best to meet these needs face-to-face. The mere filing of records, whether required by statute or not, without summarizing and analyzing, serves very little purpose other than spending money and consuming space. Keeping reports of information is only useful if they serve to provide answers to problems and guides to programs of action. In my opinion, an effective law enforcement record system should do something in terms of administrative and operational management by providing the optimum of information. This empowers an agency with the ability to provide the best law enforcement service to its community. How information is put to use in most cases serves as the yardstick which measures the effectiveness of that agency and its administration.

Information, through reports, in many law enforcement agencies, is a one-way street. The reporting process flows in and little, if any, usable information is returned to the officer on the street to assist him in the performance of his duties. With the volume of reports generated daily by

---

[1]Thomas F. Adams, Law Enforcement-An Introduction to the Police Role in the Community, (New Jersey: Prentice-Hall, Inc., 1968) p. 238.

all divisions of a medium to large size law enforcement agency, requirements for the rapid processing, analyzing, and retrieving needed information is of paramount importance.

A thorough examination of the overall aims, goals, and objectives of the law enforcement agency is a prerequisite to any efficient and effective records system.

> By study and analysis of proper police records the police department will have in its files the basic data concerning crime, traffic, and delinquency that are necessary for an intelligent plan of attack. Based on the statistical data that can be produced by a records division, the Chief of Police (Chief of Operations, etc.) will be in a position to focus the work of the police department when and where it yields the greatest immediate results. Records data will not give the solution to the crime problem. It will isolate factors concerning it so that an intelligent departmental plan of attack can be formulated. There must be developed a records and accounting system to show if the departmental operational plan of attack is producing results. Large departments need mechanical compiling and analyzing machinery to do this work. It is impossible to do it by hand soon enough, and without errors creeping into the work. Small departments use hand sorting of index cards.[2]

To derive the optimum of needed and essential information from law enforcement records the analysis and study process should include: (1) having a thorough knowledge of what information the records system should produce for the department's needs; (2) extensive use of flow charts; (3) starting from the end result in what is desired from the records system and work towards the beginning. This process eliminates the costly and time consuming trial and error method; (4) consider all the legal requirements imposed upon the department; (5) consider all interagency needs and

---

[2]Authors unknown, Administration and Use of Police Records (Course 101), (Kentucky: Southern Police Institute, date unknown) pp. 10-11 (Note: this is an unpublished course outline.)

requirements; and (6) always evaluate your budget and manpower resources.

The President's Commission on Law Enforcement and Administration of Justice noted that:

> Many departments resist change, fail to determine shortcomings of existing practice and procedures through research and analysis, and are reluctant to experiment with alternative methods of solving problems. The police service must encourage, indeed put a premium on, innovation, research and analysis, self-criticism and experimentation.[3]

Who gathers the bulk of information from the field in any law enforcement agency? Without the field officers' reports there would not be any information available to other divisions within an agency. If this occurred, obviously the reviewing, analyzing, and summarizing of information would not be possible. "Police reporting has become one of the most significant processes in modern police operations."[4]

The need for standardized and clearly defined written reporting procedures is essential to the overall administrative and operational conduct of any police department. Besides their being a permanent record of activity, reports form the basis of many administrative decisions.

> They provide a basis for budget planning and distribution of funds within the department. They are the basis for long-range planning of future needs. Reports can be used to point up needs in training in training in specific areas within the department.[5]

---

[3]Task Force Report: The Police (Washington: U.S. Government Printing Office, 1967), p. 44.

[4]Allen A. Gammage, Basic Police Report Writing, (Illinois: Charles C. Thomas, 1970), p. 5.

[5]William Dienstein, How to Write a Narrative Investigation Report, (Springfield: Charles C. Thomas, 1964) p. 3.

> Unless police agencies have a well-defined reporting policy for incidents of both criminal and noncriminal nature, they will be unable to assess accurately the extent of criminal activity in their jurisdictions, and will also find themselves ill-equipped to take effective measures against it.
>
> Moreover, inconsistent reporting procedures contribute to a lack of confidence in police; persons may well assume that certain kinds of behavior are tolerated in one section of the community but not in another.
>
> Every policeman should be thoroughly familiar with agency policy specifying the conditions under which police reports are to be taken. Such policies should require that all relevant criminal information be reported, and should discourage procedures that permit the failure to take a report.[6]

Well designed and utilized field reports are essential to any records system and especially to one that is computerized.

All of the forms used by a law enforcement agency should be designed to meet more than one need if possible. They should be practical, standardized, relatively easy to read and prepare, as well as allowing for statistical analysis summaries. Many law enforcement agencies have already placed great emphasis on their record systems and forms utilized in the collection of information. It is recommended that a review of other agencies methods be carefully examined and understood prior to any final decisions. In addition to that previously stated, the following should always be considered in forms design and development:

1. Odd-ball size forms creates an unnecessary expense upon the agency's budget when purchasing printed forms and filing cabinets, etc.

---

[6]National Advisory Commission on Criminal Justice Standards and Goals Task Force on Police (U.S. Government Printing Office, 1973) p. 571.

2. The forms designer should consider future conversion to automation when preparing a form. This eliminates costly and time consuming modification or complete re-design at a later date.
3. Use the "paste-up" method. This is when one cuts out the best of everybody else's law enforcement forms and pastes them on a piece of paper the size they want their form to be. Through this method a department can create its own forms tailor-made to meet their specific needs.
4. Consultants may be necessary as they can provide a different perspective not previously taken into consideration. However, don't overlook the talents of the people within your own departments and their experience and knowledge of that agency's operations.

Once the aims, goals, and objectives of a law enforcement agency have been set forth, the methods and procedures to achieve them must be made known to all employees. It now becomes the responsibility of the records unit to provide summarized information necessary for administrative and operational decisions. However,

> The capability of a police records staff to provide timely, accurate, and complete information to administrative and operational components of the department depends primarily upon the quality of information originally provided by its contributors. In order to insure maximum usefulness of collected information, the records element must organize the information into logical groupings that allow for the system to provide or receive information randomly and without undue inconvenience or delay.
>
> All information to be gathered, processed, stored, and disseminated falls within several major categories. It should be arranged in logical, prescribed ways to form files of retrievable data. The major categories

include:

1. FIELD OPERATIONS PRIMARY DATA:

   a. Case reports and related materials

   b. Statements and depositions

   c. Investigative notes, sketches, and similar items

   d. Evidence and property - identification information

   e. Photographs, fingerprints, and other supportive documents or records

2. FIELD OPERATIONS SECONDARY DATA:

   a. Field interview information

   b. Traffic and other violation citation data

   c. Miscellaneous information required by or for field personnel

3. FIELD OPERATIONS SUPPORTIVE DATA:

   a. Criminal history records

   b. Modus operandi information

   c. Criminal specialties file

   d. Personal identification data

   e. Wanted persons information

4. COMPLAINT AND DISPATCH DATA:

   a. Time, date, location and other information concerning incidents reported.

   b. Advisory information of immediate procedural importance to responding officers received from complaints, such as descriptions of suspects and escape routes.

   c. Information concerning officers assigned, case report numbers, and other case work-load data.

   d. Radio and teletype messages and other inter or intra-agency information sent and received.

5. ADMINISTRATIVE DATA:

   a. Comprehensive periodic reports, summaries and tabulations

   b. Case-load data on personnel and assignments

   c. Informational notices and bulletins

6. INTERNAL CONTROL DATA:

   a. Logs and registers

   b. Report review and control files

   c. Indices and cross reference data

   d. Other information required to process reports, records, and other data.[7]

To provide field and staff elements with information concerning the incidence of crime and traffic conditions, and important personnel and other data, the records element should provide both consolidated and comprehensive, daily, monthly, and annual statistical reports, special analysis of certain types of incidents, and detailed breakdowns of both statistical and analytical data. This information should be given to designated departmental elements and city and other officials or offices.[8]

Law enforcement records should meet or exceed minimum standards as prescribed by law, department policy, inter-agency requirements, Uniform Crime Reporting, and the needs of that community.

To insure that a law enforcement agency has the needed information, their records system should meet the following minimum standards:

1. A permanent written record is made of each crime as soon as the complaint is received. All reports of crime and attempted crimes are included, regardless of the value of property involved.

---

[7]Eastman, George D. and Eastman, Ester M., Municipal Police Administration (District of Columbia: International City Management Association, 1969) pp. 252-253.

[8]Ibid., p. 266.

2. Staff, or headquarters, control exists over the receipt of complaints. This is to insure that each is promptly recorded, properly classified, and subsequently counted.

3. An investigative report is made in each case. It shows fully the details of the offense as alleged and as disclosed by the police investigation. Each case is closely followed to see that reports are made promptly.

4. All reports are checked to see that the crime class conforms to the uniform classification of offenses.

5. The offense reports on crimes cleared by arrest or by exceptional means are so noted.

6. Arrest records are complete, special care being taken to show the final results of the charge.

7. Records are centralized; records and statistical reports are closely supervised by the chief administrative officer; periodic inspections are made to see that the rules and regulations of the local agency on records and reports are strictly followed.

8. Statistical reports meet the Uniform Crime Reporting standards and regulations.[9]

A suitable records system contains and can provide the following:

1. Information useful in the investigation of crimes.

2. Identification of persons and property.

3. Investigation reports [of crimes (offenses) and other matters of concern to the police] when classified, indexed, and filed.

4. Register assignments and provide a check on accomplishments so that (1) errors may be traced, (2) inadvertent oversight and willful neglect detected, and (3) successful performance assured.

5. Provide a basis for reviewing work, thus helping supervisory officers in their day to day operations by revealing deficient or improper handling of cases.

---

[9]Kelly, Clarence M., Uniform Crime Reporting Handbook (District of Columbia: Federal Bureau of Investigation, 1974) p. 3.

6. Show whether officers were correctly dispatched to the scene of criminal operations.

7. The progress of investigation.

8. Failure to follow up on investigations or otherwise correctly dispose of police business are revealed.

9. Prevent the individual policeman from conducting an investigation or discontinuing it in violation of departmental policy and sound police practice.

10. Enable the police department to disprove charges of improper police action by providing prompt and complete answers to specific allegations and inquiries from the administrative head of the city, citizens, etc.

11. Records and summary reports will give a picture of present conditions and problems faced by the department, of the work of individual employees, activities of units, etc., in dealing with these problems.

12. Reveal significant changes in criminal and other activities requiring police attention.

13. Prompt analysis of police records guide the police official in meeting unusual needs.

    a. The first step in solving a problem is to diagnose it. Facts concerning the character, location, time, circumstances of crime and incidents requiring police action can be found.

    b. Possible to determine engineering, education and enforcement needs pertaining to traffic.

    c. Locate and identify police hazards, isolate the locations requiring attention.

14. Assistance in the development of police strategy and in making various follow-through procedures.

15. The success of programs launched to lower crime and accident rates can be ascertained by record analysis.

16. Provide measuring sticks or indices to appraise police efficiency and accomplishment.

17. Effectiveness of police policies and procedures, and the results of changes in methods of operation may be appraised.

18. Information for public dissemination is made readily available through a suitable record system.

19. Supplying information useful in preparing and supporting budget estimates.

    a. Assist in managing the department's fiscal affairs.

    b. Accurate payrolls compiled.

    c. Competing with the programs of other city departments for public funds can be justified.[10]

As a law enforcement information system increases in size and volume, the need for some form of automated system becomes necessary for the effective management and control of that information. Should an agency have need for automating its records system, the following should be given careful and serious consideration.

An operating law enforcement system should be established to serve: "(1) daily operations, (2) investigative analysis, (3) management analysis, and (4) program formation."[11]

It should be emphasized that the use of automated data processing is a management tool. The computer is by no means the answer to every law enforcement agency. The quality, integrity, and accuracy of computerized information is only as good as those human beings who write the data collection

---

[10]Authors unknown, Administration and Use of Police Records (Course 101), (Kentucky: Southern Police Institute, date unknown) pp. 10-11 (Note: this is an unpublished course outline.).

[11]John H. Parsa, "An Automated Police Information System for a Small Town," Diss. Texas Tech University, 1972, p. 8.

reports, key punch the information, and program the computer to print the needed information in usable form. Once high standards have been established, the rapid retrieval of information becomes almost commonplace. Decisions in a law enforcement agency have to be made rapidly.

Automation provides this capability; not subject to vacations, regular days off, and coffee breaks, but operating rapidly, accurately, and efficiently to provide indicators and guidance in decision making. It is impossible to do it by hand soon enough, and without errors creeping into the work.

> Automated information systems make it easier to collect, process, and communicate data; but they cannot be expected to exercise responsible judgment. Any tool that facilitates the collection and organization of data in a complicated and changing fact situation is a significant aid to judgment. Of course, computers are useful in assembling the facts on which to base a decision. Computers can provide no substitute for the process of judgment based on experience. The electronic revolution offers the creative police administrator and field officer greater scope, as it makes available more data, assembled more rapidly, from a wider geographic range of sources, and more easily combined and recombined.[12]

A law enforcement information system, while safeguarding the rights to privacy of individuals, can effectively provide important indicators to other local, state, and federal agencies in the performance of their responsibilities. See Figure 1, Interprofessional Opportunities.

> Success in protecting society is not measured by the length of time it takes the police to respond to a crime scene, by the number of arrests they make, or by the number of arrestees successfully prosecuted or

---

[12]Paul M. Whisenand and Tug T. Tamaru, Automated Police Information Systems (New York: John Wiley and Sons, Inc., 1970) pp. 198-199.

Figure 1. Interprofessional Opportunities

SOURCE: IACP Training Key Number 139, 1970

INTERPROFESSIONAL OPPORTUNITIES

By Contacting:	You May Influence and Help to Coordinate:
City or County Planning Department	Comprehensive planning (security aspects of public buildings, shopping centers, high rise apartments, etc.)
Civil Defense Office	Disaster plans and emergency operations
Courts	Other than in specific criminal cases, legal advice on police procedures; handling of juveniles; availability of juvenile or probation specialists, handling of alcoholics
Building and Safety	Reduction of attractive nuisance hazards, abandoned buildings, etc.; establishment of minimum physical security standards
Fire Department	Arson investigations; crowd control needs; disaster responsibilities; fire prevention techniques at accident scenes
Health Department	Alcoholism problems; communicable disease control; drug use and abuse; pollution violations; prostitution and venereal disease control; public sanitation violations
Licensing Agencies	New businesses (owner, location, etc.) Door-to-door solicitors; liquor law enforcement
Parks and Recreation Department	Recreation area supervision; recreation programs and personal safety of participants; "Lovers' Lane" problems
Public Works	Street and alley lighting requirements; trash regulation enforcement; "littering" problems; snow removal needs
Street or Highway Department	Removal of abandoned vehicles; driveway requirements; parking controls; pedestrian control; traffic flow; high accident intersections (engineering changes), etc.
Schools (The school board itself and in your area)	Counselling and guidance in areas of police concern; delinquency control programs; educational programs (narcotics, safety, child molesters, etc.); vandalism control; internal patrol responsibilities, truancy and youth gang control
Welfare Department	Assistance to persons in need, especially on an emergency basis; family counselling; aid in locating missing persons, etc.

sentenced. Rather, success or failure is determined by the degree to which society is free of crime and disorder.

> This is but another way of saying that no element of the criminal justice system completely discharges its responsibility simply by achieving its own immediate objective. It must cooperate effectively with the system's other elements. This requires an effort on the part of each element to communicate with the other elements, which is sometimes difficult because of legal and administrative separation of powers and responsibilities.[13]

A law enforcement information system, properly administered, can serve many needs; from the chief or sheriff, the prosecutor, the crime analyst, and the criminal justice planners to name a few. However, one fact remains very clear. It is this:

> No one program alone can deal effectively with crime and delinquency. The home, the school, the church, the welfare agency, the clinic, the police, the court, the probation department, the correctional institution, the parole agency, and all the other agencies and institutions that are interested in crime and delinquency must work together as a team through coordinating councils or through some similar coordinating device in a concentrated attack on these problems. But the teamwork cannot be completed without public support. This support must be given in the form of interest in community affairs, participation in community programs, law observance, insistence on wholesome community conditions, and abundant opportunity for young people, respect for law enforcement and effective court procedures, demand for an adequate number of well-qualified police officers, judges, probation officers, welfare workers, institutional employees, and parole officers, and a willingness to pay for programs that can deal effectively with social problems.[14]

---

[13]National Advisory Commission on Criminal Justice Standards and Goals, Police (Washington: U.S. Government Printing Office, 1973), p. 70.

[14]Robert G. Caldwell, Criminology, 2nd Ed., (New York: The Ronald Press Co., 1965) p. 724.

BIBLIOGRAPHY

Books

Adams, Thomas F. Law Enforcement-An Introduction to the Police Role in the Community. New Jersey: Prentice-Hall, Inc., 1968.

Authors Unknown. Administration and Use of Police Records (Course 101), (Kentucky: Southern Police Institute, date unknown) pp. 10-11. (Note: this is an unpublished course outline.)

Caldwell, Robert G. Criminology, 2nd Ed., New York: The Ronald Press Co., 1965.

Dienstein, William. How to Write a Narrative Investigation Report. Springfield: Charles C. Thomas, 1964.

Eastman, George D. and Eastman, Esther M. Municipal Police Administration. Washington: International City Management Association, 1969.

Gammage, Allen A. Basic Police Report Writing. Illinois: Charles C. Thomas, 1970.

Kelly, Clarence M. Uniform Crime Reporting Handbook. District of Columbia: Federal Bureau of Investigation, 1974.

Parsa, John H. "An Automated Police Information System for a Small Town." Diss. Texas Tech University, 1972.

Whisenand, Paul M. and Tamaru, Tug T. Automated Police Information Systems. New York: John Wiley and Sons, Inc., 1970.

Public Documents

National Advisory Commission on Criminal Justice Standards and Goals Task Force on Police. U.S. Government Printing Office, 1973.

Task Force Report: The Police, Washington: U.S. Government Printing Office, 1967.

FLOWCHARTING

The successful solution of a problem, whether manually or on an electronic computer requires completion of three main "solution" steps. First, the problem and desired results must be completely understood; next, the solution to the problem must be logically designed; finally the necessary tasks to solve the problem are undertaken. The first two steps of a solution are especially important. They may be considered independent from the third and completion may be demonstrated by a flowchart.

A flowchart is a graphical representation of the step-by-step solution of a problem and aids the problem solver by clearly defining what task should be accomplished and at what time.

Communication of ideas and techniques are aided greatly by flowcharts. This is particularly true if one is trying to explain a problem's solution to another person not familiar with terminology or procedures. For example, a crime analyst may have designed a solution to a particular problem and wants a computer programmer to place this solution on an electronic computer. A well written flowchart defining this solution is almost a necessity for the successful translation of the analyst's ideas into a computer program.

The flowcharted solution of a simple problem is illustrated in Figure 1. Figure 2 provides the standard shapes of symbols used for flowcharting, along with a brief description of the use of each.

As demonstrated by the flowchart in Figure 1, problems solved using flowcharts do not always require processing of data. Most that do, however, have similar operations of data input, data processing and data output. Since most flowcharts are written to process several sets of input data, loops are generally set up to input the next set of data if the processing is not complete. Figure 3 illustrates a typical data processing flowchart example.

Example and Problems

Assume that you are analyzing data on burglaries and that data is available on file for each case as shown in Table 1. Figure 4 shows a flowchart of finding the total number and compiling a list of all burglaries in Sector 2 occurring between 9:00 p.m. and 11:00 p.m.

Solve problems 1-5 using flowcharts, assuming data is available as shown in Table 1.

(1) List all burglaries that occurred in the city between January 1 and February 15.

(2) List all single family burglaries from Section 4 between April 1 and April 10.

(3) Find the total number of burglaries in Section 1.

(4) Find the average number of burglaries that occurred during January in Sector 4.

(5) Find the number of multi-family burglaries in each sector for the month of February.

Table 1

Data Available	Description
Sector	Sector of city between 1 and 8.
Address	Street address of burglary
Type of Residence	Single family or multi-family
Date	Day, month and year of burglary
Time	Hour and minute of burglary

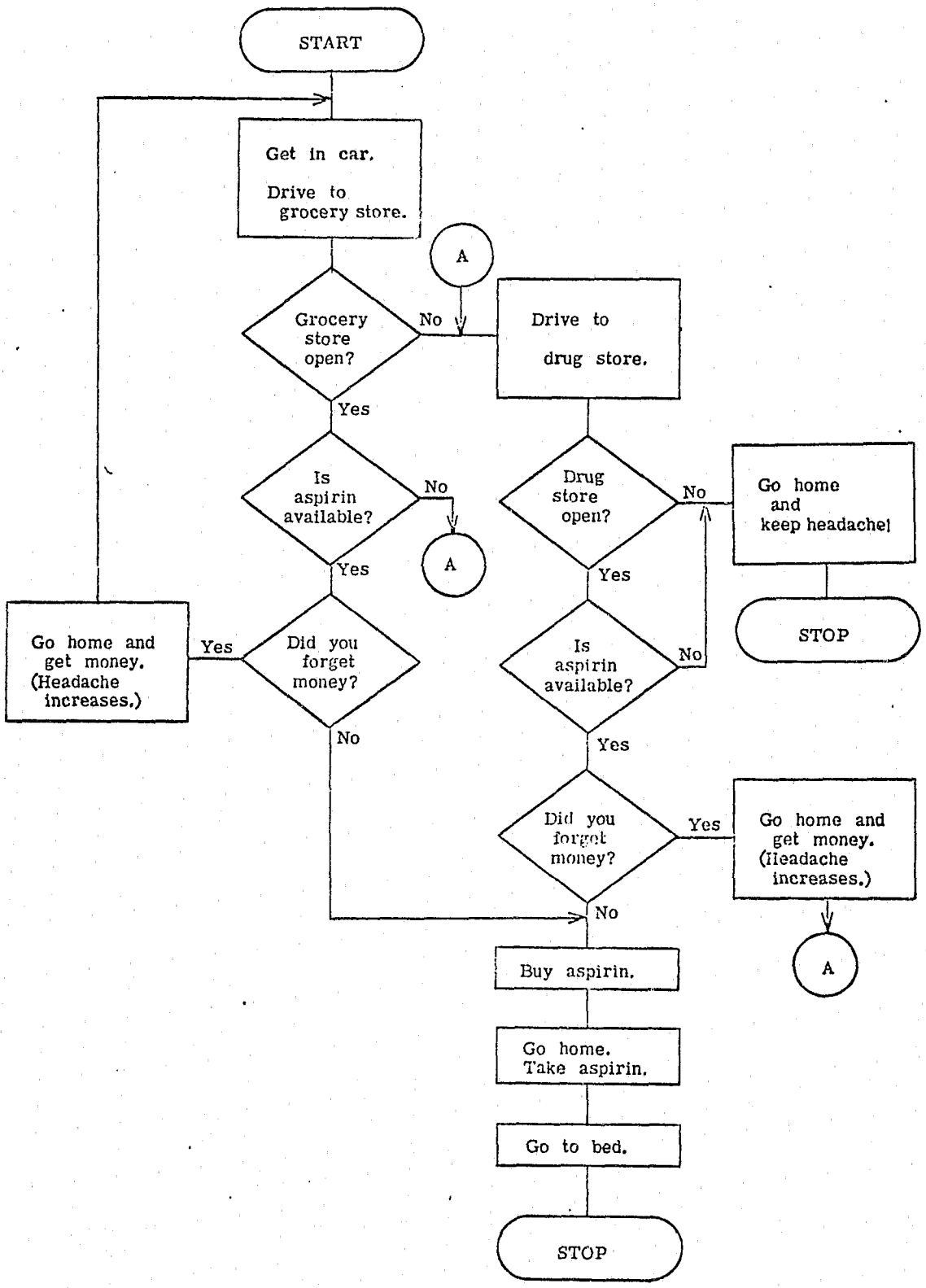
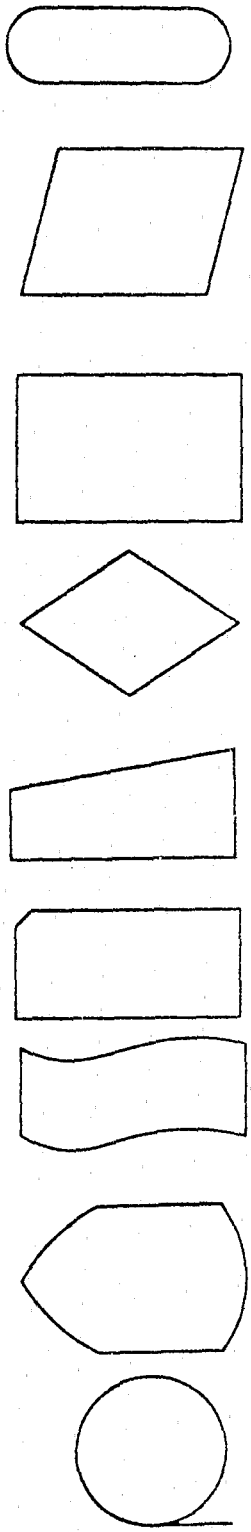


Figure 1 Example of Flowcharting Technique



A terminal point; the first or last item in a chart or in a subroutine.

Input/output; by previously determined means, such as keyboard, tape, line printer, etc. Additional symbols are used (see below) to specify a particular medium.

Predefined process or comment; indicates an operation or definition of variable, or a programmer's relevant comment, usually in dotted structure.

Decision; allows insertion of a decision-making apparatus, as in interval selection, counter comparison or update, loop exit, etc.

Manual input; usually by keyboard, a supplement to above "input/output."

Punched card

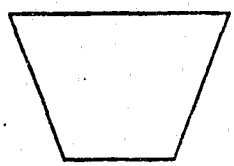
Punched tape

CRT display

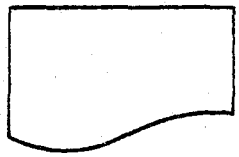
Additional symbols for specifying a particular medium of input or output.

Magnetic tape

Fig. 2 Standard Flowcharting Symbols



Manual operation; any operation performed externally to an existing machine set-up, done by the operator or other personnel.



Document; sometimes used to designate a "hard-copy" output; any printed item used for input or output.

On-page connector; used to allow flow lines to continue where otherwise they would cross; must be coded, such as "a1," and should be placed so as to flow down or to the right.

Off-page connector; used in multi-page charts to continue a flow line; must be coded appropriately, including page from which or to which continued.

On-line storage; any medium used as intermediate storage.

Magnetic disc or drum; used for a specifically assigned storage.

Fig. 2 Continued

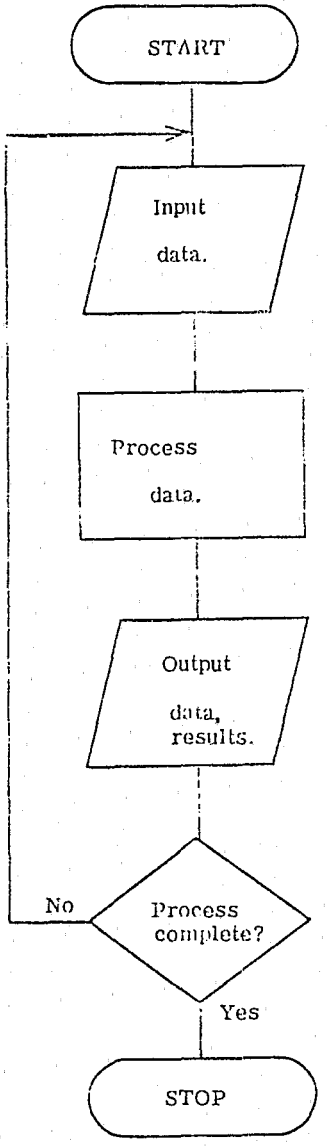


Figure 3 A Typical Flowchart

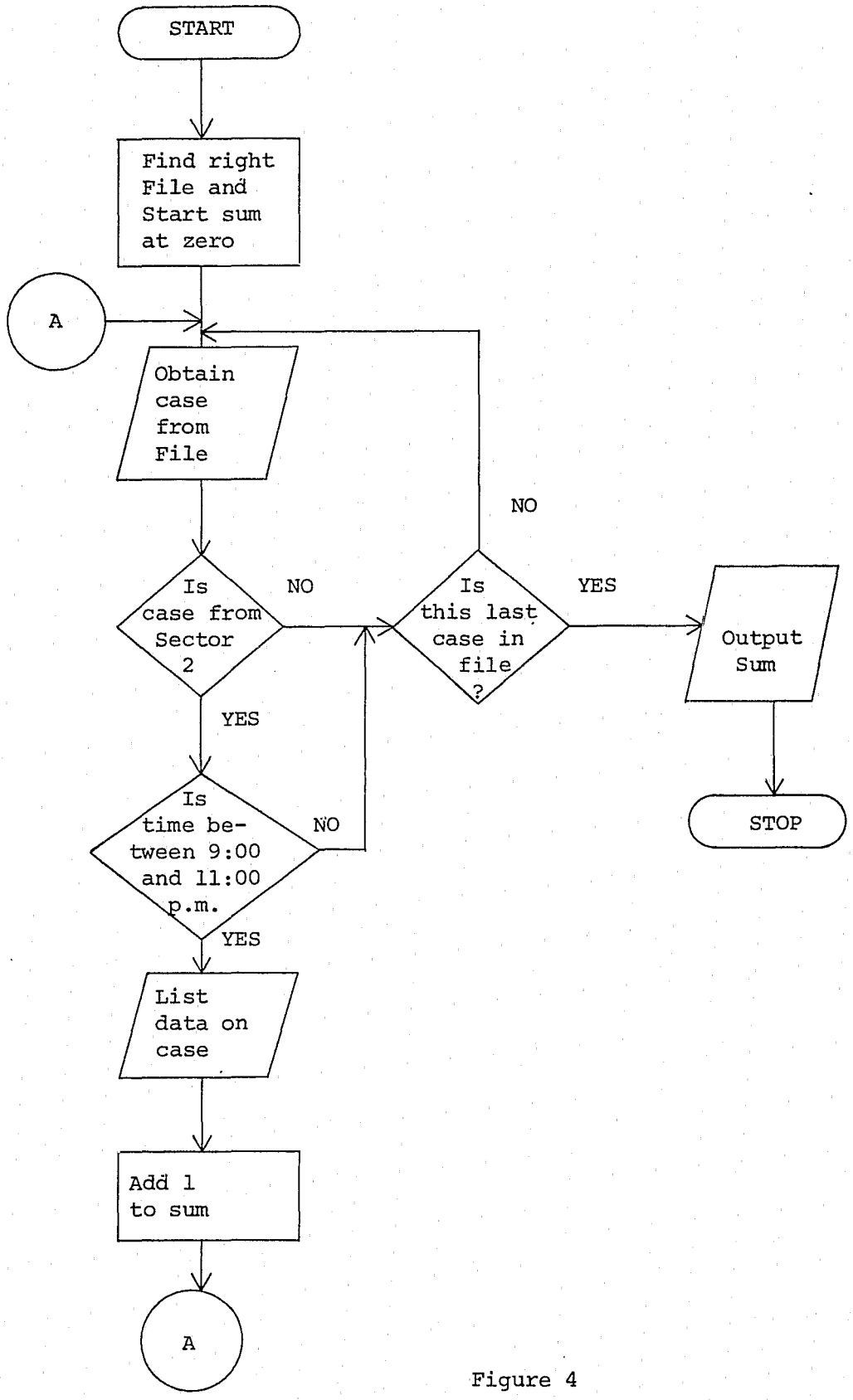

START
Find right File and Start sum at zero
A
Obtain case from File
Is case from Sector 2
NO
YES
Is time between 9:00 and 11:00 p.m.
NO
YES
List data on case
Add 1 to sum
A
Is this last case in file ?
NO
YES
Output Sum
STOP

Figure 4

THE USE AND MISUSE OF STATISTICS

The crime analyst will be primarily interested in performing four major functions related to crime data:

(1) collection
(2) organization
(3) analysis, and
(4) interpretation.

The accomplishment of these four functions is a science generally referred to as Statistics. Statistics does not then refer to large complicated formulas or technical sounding names and terminology. So often use of terms like "regression analysis", "correlation coefficients", "analysis of variance" turn people off simply because they do not understand their meanings. They, therefore, assume statistics is too complicated and, therefore, worthless. We will then start our discussion of statistics with a warning - do not try to impress people with terminology and formulas. Remember that these formulas, etc., fit into only one of the four functions of statistics, analysis, and, even though these formulas are important and necessary at times, you should use analysis techniques that are easily explainable and helpful to accomplish the fourth function of statistics, interpretation.

The first two functions of statistics, collection and organization of data, is accomplished by a well organized reporting scheme as discussed in previous sections. The fourth function, interpretation of crime data, will be discussed later. In this section we will concentrate on some simple techniques of statistical analysis.

Data and Sampling

Before data is to be analyzed, the way it was collected and organized must be studied. For example, if you are to analyze the frequency of burglaries, you should make certain the data on burglaries has been accurately filed. Moreover, if for instance you want the average number of burglaries per month, you would not take only the data from the month of November and December. Two major errors would be made.

First, the data is not independent and representative. Burglaries are generally more frequent during these months. Also, the sample taken is too small. The weight one can place upon statistical estimates is directly related to the independence of data and sample size. It would be quite simple to "prove" that average daily rainfall for Texas is .5 inches if I only measured the rainfall in San Marcos during the first week of May.

One should make certain that the data is accurate and representative before performing analysis and should remember that small data samples can be most misleading. Sample sizes should always be represented so that the proper significance can be placed on the results.

Averages

Before using the term "average" one should remember that there are different types of averages, and each type may lead to a different interpretation of the data. The mean or arithmetic average is generally most familiar and used most often. The mean salary of a group of individuals is simply the sum of all salaries divided by the total number of individuals.

The median of a set of data is that point on a scale of measurement where an equal number of cases are on each side of it -- half are above and below the median. For example, the median of the numbers 10,8,8,7,6,5,5,5,0 is 6 since 4 numbers are larger and 4 smaller.

The mode is that measurement or piece of data that repeats most often. For the example above, 5 is the mode since it repeats most often.

An analyst should use that "average" which is most meaningful for the data being considered. For example, assume data on value of property stolen is given as in Table 1. Out of 15 items stolen the arithmetic average of $6,243.33 gives a fair idea of the total value stolen, but not a good idea of the types of items. Perhaps the median of 300 or the mode of 10 would better communicate the desired meaning.

TABLE 1

Item	Value of Item in Dollars	
1	50,000	
2	40,000	6243.33=MEAN
3	1,000	
4	700	
5	500	
6	500	
7	400	
8	300	MEDIAN
9	100	
10	100	
11	10	MODE
12	10	
13	10	
14	10	
15	10	

Graphing

One of the best visual aids one can use to represent data (but not interpret it) is that of graphing. The quantities graphed are generally referred to as variables, or things that vary in value from case to case. The number of times a value of a variable occurs is referred to as that variable's frequency. A distribution is a set of values for variables that are ordered according to magnitude of a variable.

There are two primary graphing techniques for distributions of data, histograms or polygons. In graphing in two dimension, there are always two variables under consideration. For example, a monthly burglary rate is shown in Figure 1, where one variable (independent), the months of the year, are in increasing order while the other variable, the number of burglaries in the month, are dependent on which month is being considered. The histogram generally uses the upper and lower limits of an interval and the entire interval is plotted on the graph.

Keep in mind that any visual aid is used only as a means of analysis and does not interpret the data. Interpretation must be accomplished by someone familiar enough with the data to determine if the results are significant. Figure 1 can be used in conjunction with our discussion on complete data samples. Let's assume that we consider the sample size large enough to make estimates of burglary trends. If one considers only the months of January - May, one might predict a fantastic decrease in

burglaries. This, of course, is incomplete data samples, since the summer and holiday (December) months are typically bad as far as occurrences of burglaries are concerned.

A polygon is a graphic method which uses points to represent frequencies, with lines connecting these points. Figure 2 is Figure 1 redrawn as a polygon.

One final example of how figures, say polygons, can be drawn to be somewhat misleading is shown in Figures 3 and 4. Assume Figure 3 is a graph of the monthly expenditures for crime prevention during the past year. While the expenditures have increased, relatively, this increase was small. Figure 4 represents the same data, but notice that the scale has changed significantly, implying a fantastic increase in expenditures. Care should be taken when constructing graphs, and when interpreting them, to make sure the graph is not misleading.

Correlation

Correlation is a measure of the relationship occurring between two variables. The simplest type of correlation study is graphical linear correlation. Two variables, say truancy and number of burglaries are plotted on a graph so that the number of truancies is in increasing order. (Measurements are graphed then according to say weekly truancies and weekly burglaries.) Figure 5 shows this graph. Notice that as truancies increase, so do burglaries. We, therefore, say there is a correlation, and since the data appears to be on a straight line, there is linear correlation.

If the plot appears to have no relationship, or if the straight line is a horizontal one, no correlation is present. See Figure 6.

Figure 7 shows a correlation such that as one variable increases, the other decreases. This is referred to as negative correlation since the straight line has a negative slope. Figure 5 was an example of positive slope or positive correlation.

A general equation of a line is given by $y = mx+b$ where x and y are the variables, and m is the slope. The values m and b may be computed for any sample of data so that the straight line can be computed. The reader is referred to texts in the bibliography or any introductory statistics book for these formulas.

Keep in mind that correlation does not necessarily imply that one of the variables causes or even affects the other. For example, one

might examine the correlation between temperature and number of petty thefts. It might appear that as temperature goes up, so does petty theft. They are, therefore, related. However, one certainly cannot assume that the rise in temperature caused the rise in thefts. Instead, it could be the fact that school is not in session during the summer months that explains the increase. In other words, the correlation between two variables may be caused by a third variable. Care should therefore be taken on interpreting correlation graphs, although their uses are of extreme importance.

Questions to Ask

As a matter of summary, we end this section with three questions which should be asked whenever performing analysis, or reviewing someone else's results and conclusions.

1. How reliable is the data?

   Make sure the data was acquired and reported accurately and independently. Make sure there is no built in bias. For example, was data collected only in one area, say, to make someone "look" good? Finally, make sure the sample size was large enough to perform a reasonable analysis.

2. What is the best way to present the data?

   Remember that many people will be interested in your data and many may aid in the process of interpreting your data. Thus, choose the presentation technique which best fits your audience and which best represents your data.

Remember that your mode of presentation may greatly affect interpretation as was demonstrated in Figures 3 and 4.

3. Does the result make sense?

Always remember that the fourth function of statistics is interpretation and that ultimately some conclusions will be reached. Make sure that the results are reasonable! If they are not, perhaps one of the four steps of collection, organization, analysis and interpretation of the data had a flaw which led to the unrealistic results.

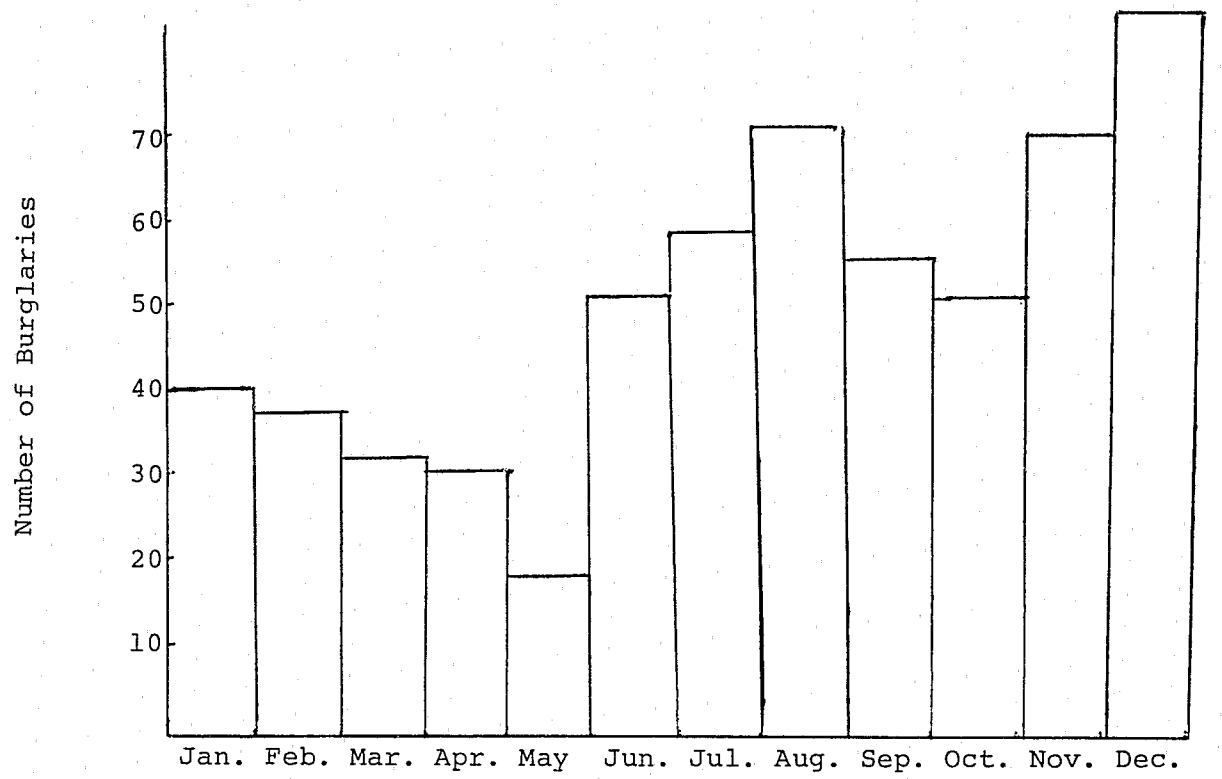


Figure 1

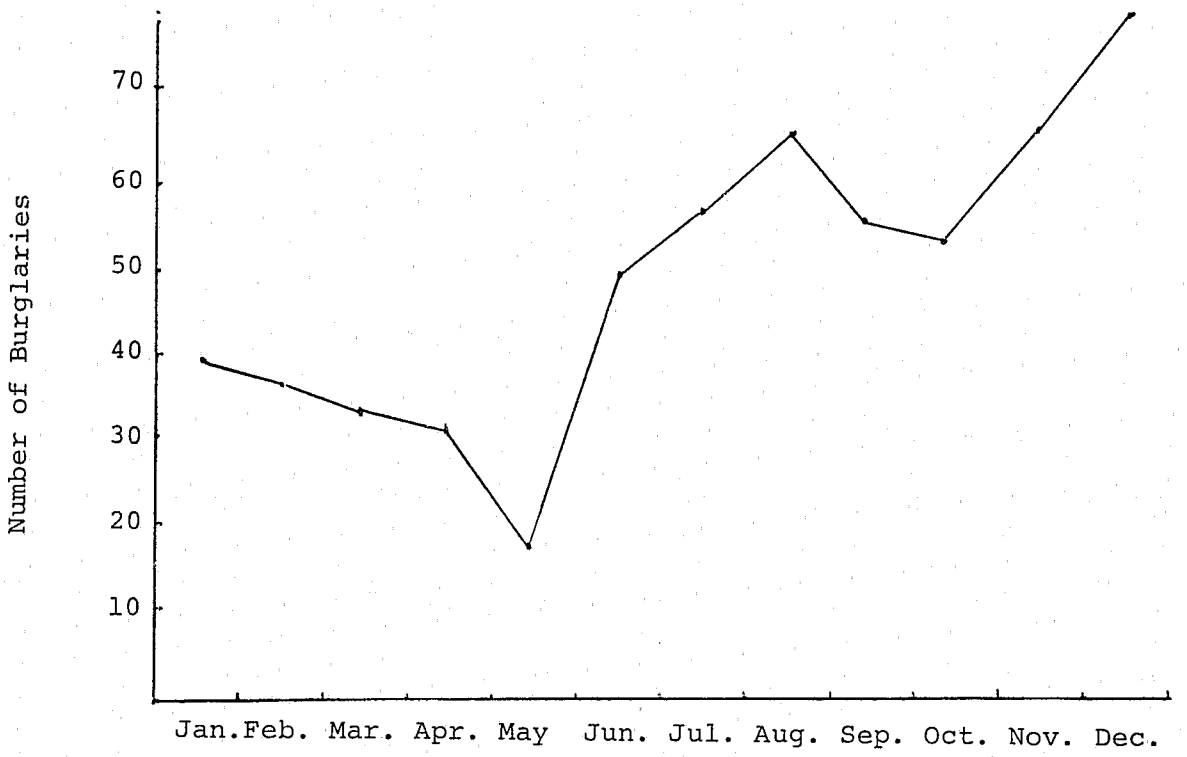


Figure 2

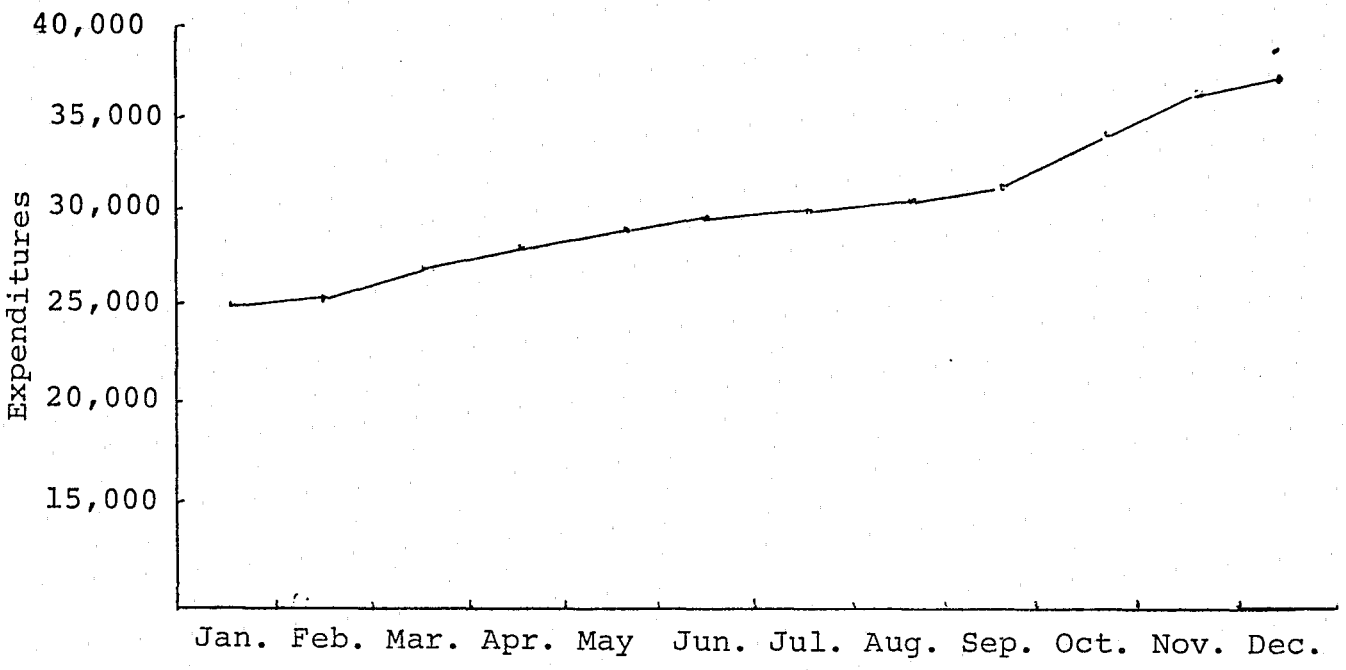


Figure 3

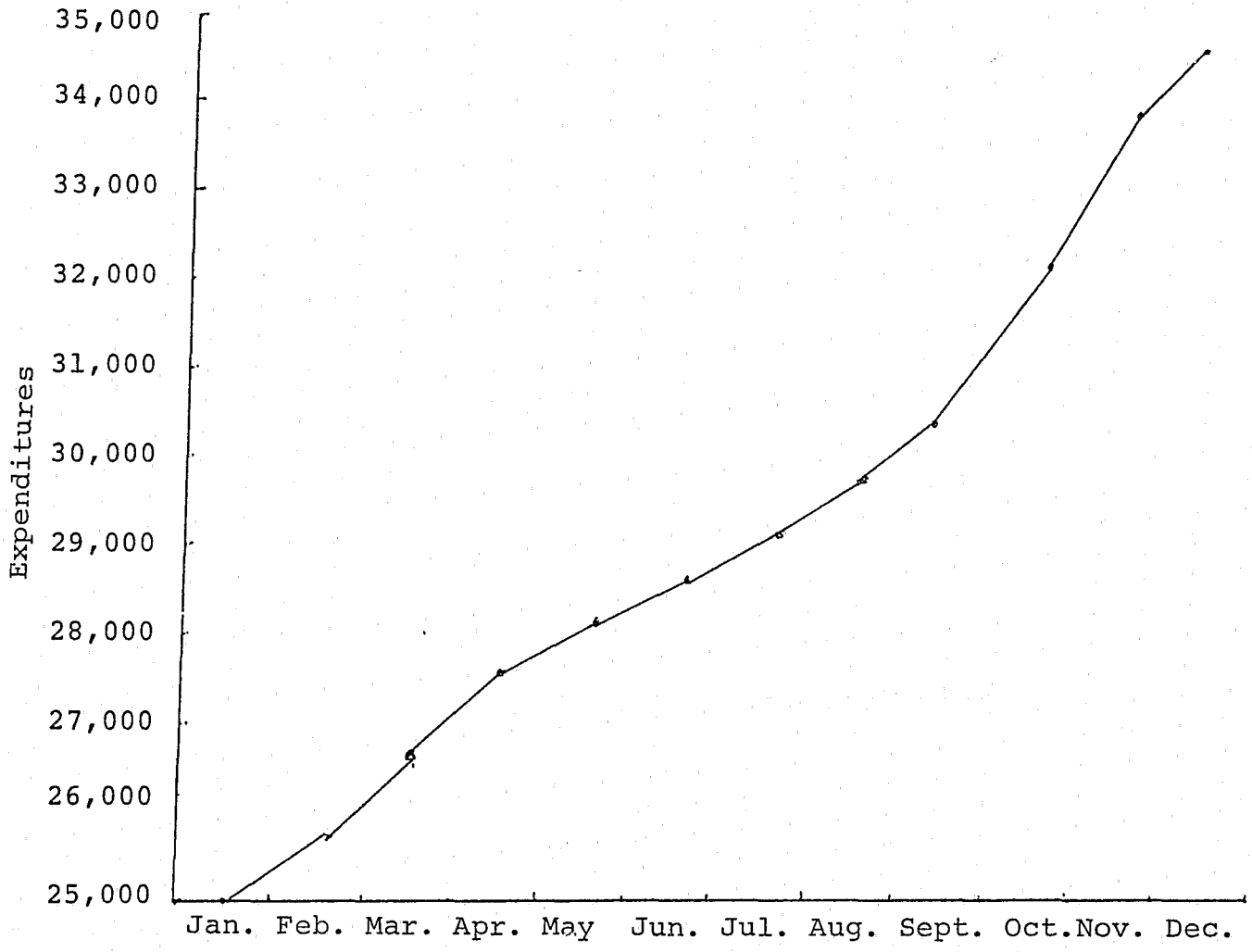


Figure 4

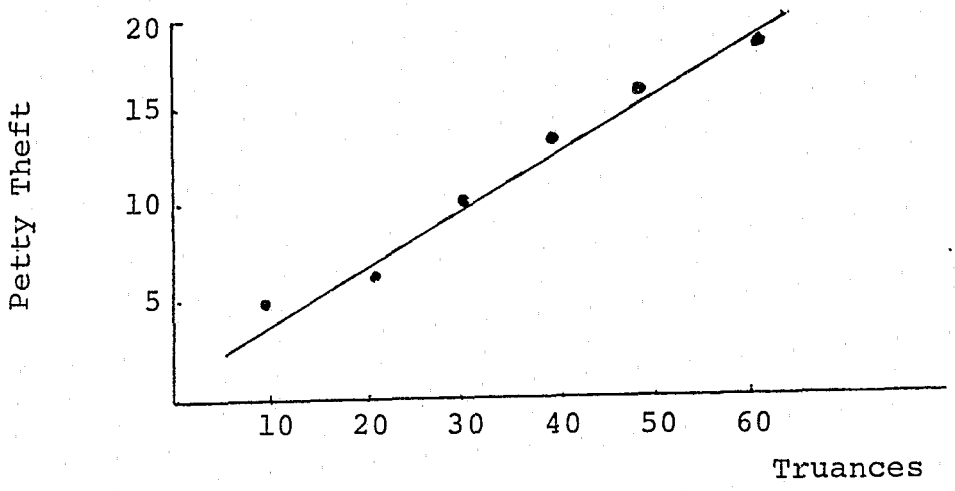


Figure 5

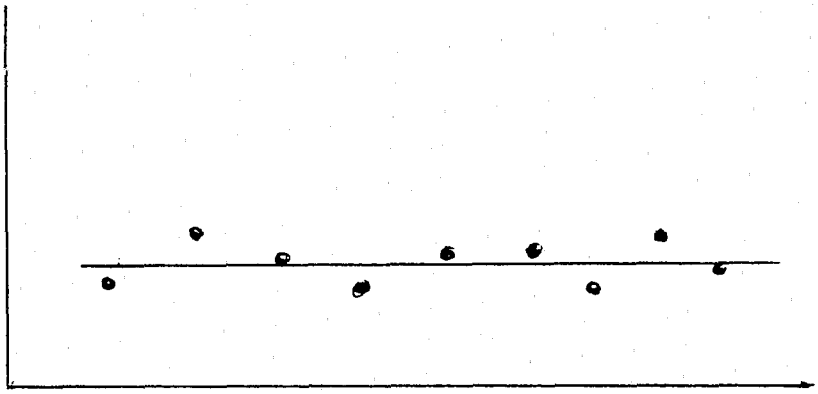


Figure 6

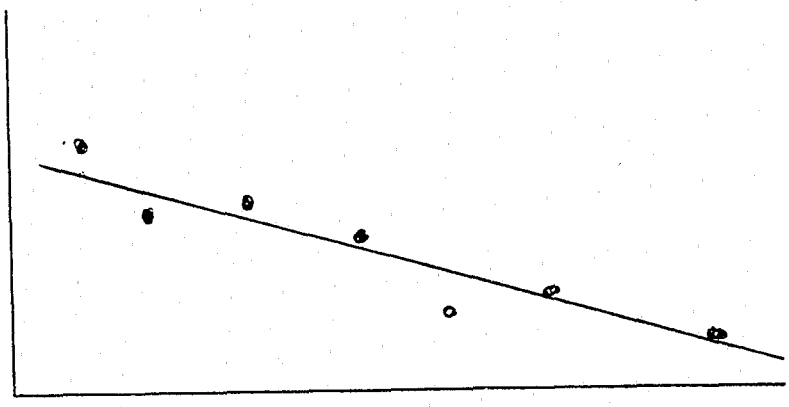


Figure 7

BIBLIOGRAPHY

Huff, Darrell. How to Lie With Statistics. New York: Norton & Co., 1954.

Ingram, John A. Introductory Statistics. Menlo Park, California: Cummings Publishing, 1974.

Lindgren, Bernard W. Basic Ideas of Statistics. New York: MacMillan Publishing, 1975.

McCauley, R. Paul. Crime Analysis. Louisville, Kentucky: The National Crime Prevention Institute.

ANALYSIS OF CRIME DATA

This section will deal specifically with actual crime analysis. However, before functional crime analysis can be accomplished, the analyst must know something about the area in which he is working whether the analyst is responsible for crime analysis in a whole city or in the case of a large city, only a particular section of the city, he must have the same basic tools. The following are elements that might be helpful to know before analysis is begun:

Population of the City and Selected Subdivisions. The total population of the city and designated sub-areas such as neighborhoods, census tracts, planning areas or beat areas should be noted. This information will be useful in calculating crime rates per population size.

Median Value of Houses and/or Household Income. Document the housing values or income levels for the total city and sub-areas. This information can be used as an estimate of property values and affluency so as to provide, for example, guidelines for magnitude and type of security improvements economically feasible.

Housing Units by Type for the City and Designated Sub-Areas. Determine the total number of housing units by type (such as single family, multi-family, etc.) for both the city and designated geographic sub-areas. This data will serve as a base

to compare crime statistics. It will also be useful in the design of the prevention approach.

Number of Commercial Establishments by Type. Document the number and type of commercial establishments in the city. It would be desirable to be able to block out the geographic location of principal commercial concentrations in the city by type. This can be used to focus program activities and determine opportunity levels for criminal activity.

Population for City and Selected Subdivisions by Sex and Age. This can be used to help identify portions of the community with groups of potential offenders; i.e. young males.

Median Education Levels for City and Selected Sub-Areas. This can be used to focus a program by providing a perspective as to how sophisticated the techniques and/or materials should be understood by various groups in the community.

Non-English Speaking Persons by Native Language for City and Selected Sub-Areas. This can be used to help prepare public education materials if such items will accompany the project to be undertaken.

Median Rental Costs for City and Selected Sub-Areas. This will provide information as to the type of security improvements

that might be suggested in such units.[1]

Many others can easily be added to these and as the analyst familiarizes himself with the area he is working, he will add additional characteristics of the area to his data base such as seasonal trends and additional general facts about population makeup.

There are four basic steps to data analysis. These are collection, organization, analysis and interpretation.

Collection and Organization

The first step in collection and organization is determining what data to collect. The following are data elements most necessary to crime analysis:

- Classification of the Offense - What type of crime is it? i.e. Residential Burglary, Business Burglary, Construction Related Burglaries and Thefts? Once this determination has been made, the different crimes should be put in a specific crime category.
- Location of Occurrence - What district or beat did the crime occur in? What is the exact address of the location of occurrence? i.e. Burglary of a Vehicle-District 22-1616 Main Street.

---

[1]An Operational Guide to Data Development and Analysis for Crime Prevention Program Administration, Koepsell-Girard and Associates, Inc., 1975.

- Time Analysis - These elements should include time of day of occurrence, day of week of occurrence, exact date(s) of occurrence and time, date, and day of week that the crime was reported to the law enforcement agency.

- Method of Entry, Method, or M/O - Information captured here should tell how, if known, the crime was accomplished.

Method of Entry

(1) In the case of a residential burglary, the analyst would be interested in how entry was gained. It could have been through an unlocked front door, by kicking in a rear door, through an open garage, etc.

Method

(2) In the case of a theft where there is no breaking and entering involved, the analyst should be interested in how the theft was accomplished. i.e. Offender removed lumber from an unsecured construction site.

M/O

(3) In the case of robbery, the analyst is interested in what the offender did to accomplish the act of robbery. i.e. The offender walked in the front door of the store, pulled a .22 caliber revolver, and made verbal demand of money.

- Type of Property Taken - Identify what type of property (i.e. money, furniture, auto accessories, etc.) was taken in the particular crime category he is analyzing.

- Value of Property Taken - This information is important for several reasons:

(1) Determining the seriousness of the problem.

(2) Good information to use in Crime Prevention Presentations.

(3) Useful for state and federal reports as well as crime studies.

- Suspects and Suspect Vehicles - This information is needed for apprehension as well as determining what type individuals are commiting the crime. i.e. young people, adults, truants, etc.

Trend Analysis

There are four basic questions the crime prevention analyst should ask when determining crime trends. These are:

(1) Where is the crime occurring?

(2) When is it occurring?

(3) Why is it occurring?

(4) What can be done to aid in prevention?

From the data collected and organized, the crime prevention analyst should be able to answer these questions. From data collected by location, a determination can be made as to general geographic location of occurrence and also pin-point exact locations.

An analysis of when the crime is occurring will be more difficult in some of the crime categories (i.e. burglaries), due to the fact that the reported time of occurrence of some crimes may range from an hour,

a day, two days, a week, or more time span. A possible way of approaching this is in the actual analysis, throw out the extremes because they tell you very little as far as actual time of occurrence and consideration of them may skew your results.

The answer to the question of "why the crime is occurring" may not be answerable. Depending on the particular type of crime being analyzed answering these questions may help in determining "why" and also aid in prevention.

- Are residences and businesses being burglarized because citizenry do not take proper precautionary measures. (How is entrance being gained?)
- Do you have a truancy problem? Could part of your burglary and theft problem be contributed to juveniles who are also truant?
- Is manpower being deployed adequately from your law enforcement agency to the problem areas?
- Is an effort actively being taken to educate citizenry in the use of good preventive equipment? (i.e. locks, etc.)

Interpretation

The most serviceable interpretation of any analysis is one which considers all indicated variables. This may be positive consideration (include that data in the analysis and provide explanation for it in the interpretation) or, negative consideration (exclude that data in the

analysis and provide justifiable explanation for its exclusion in the interpretations).

Example:

Given a set of sixteen residential burglaries, you've done a time analysis on their probable times of occurrence and all but two of the burglaries fall within a forty-eight hour time span.

If you considered all the burglaries your time span would be one week. Obviously, the best solution is to consider the fourteen burglaries falling in the forty-eight hour span for the most probable time of occurrence and reference the two exceptions.

The above example lends itself to time analysis, but the same criteria are useful in interpreting location, method and/or M.O., probable target, and property on either expanded or condensed scales, depending on the type analysis you are interpreting.

Remember, interpret only what the data analysis and experience tells you. The analytical techniques you have at your disposal, the experience you quickly gain with practice and from contact with others in your field.

SUGGESTED READINGS

Police Crime Analysis Unit Handbook, George A. Buck, Project Director, November, 1973.

An Operational Guide to Data Development and Analysis for Crime Prevention Program Administration, Koepsell-Girard and Associates.

COMPUTER DEVELOPMENT*

It is difficult to find an individual in our country who is not directly or at least indirectly influenced by the electronic computer. Obvious daily computer usage is found in payroll checks, utility bills and department store check-out stands. The effect the computer has had on society has been fantastic, and yet misunderstandings and even fear of the computer is prevalent among this same society. The majority of these fears are generated by ignorance of the computer and its operation. In turn this ignorance has been caused for the most part by the rapid development and widespread usage of the computer during the last 25 years. The majority of this country's population was educated prior to the introduction of computer related curriculum in our school systems.

A crime analyst may not have a computer system immediately available for use. With the rapid development and implementation of computer systems, however, there is little doubt that sometime in the near future, all analysts will either obtain data and results from or actively use a computer facility. It is therefore important that an analyst not only have some idea of what a computer system is and how it functions, but also have some knowledge of the historical development of computers.

*Taken in part from: James L. Poirot and David N. Groves, Teaching Computer Science in the Secondary School, Southwest Texas State University, 1975.

A Brief Historical Overview

The progress of business data handling might be yet in the rock-counting state were it not for the development and use of the abacus.[1] The idea of a mechanical device with the capability of aiding in the handling of numerical data is the driving force behind the current inundation by various machines.

No particular link is necessary between the actual mechanics of one machine and those of another, in order to consider one the forerunner of the other. The search for more rapid and accurate means to an end is the element that connects the abacus to Napier's Bones to the IBM 370.

Napier devised a means of using tabular information placed on a mechanical device to facilitate the solution of certain problems. Only mechanical detail and sophistication separate his rude instruments from Bollee's direct multiplication using tabular multiplication information on wheels.

Of all the mechanical approaches to calculation, including those of Pascal and Leibnitz, the engines conceived by Charles Babbage are without doubt the most sophisticated and ingenious yet devised. Even today the accurate construction of the "Analytical Engine" would tax a well-equipped machine shop and structural engineer.

---

[1]The historical references used here and in the "Selected Chronology" are based in part on scattered references in these works: James W. Estes and B. Robert Estes, Elements of Computer Science (San Francisco: Canfield Press, 1973), chap. 10 passim; Matthew Mandl, Fundamentals of Electronic Computers: Digital and Analog (Englewood Cliffs, N. J.: Prentice-Hall, 1967), pp. 4-6; and D. D. Spencer, Computers in Action: How Computers Work (Rochelle Park, N. J.: Hayden, 1974), chap. 2 passim.

The contributions of Burroughs, Powers, Felt, Odhner, and Monroe follow closely the ideas of Pascal and Leibnitz, in that they devised ingenious mechanical devices for handling numerical data. None, however, approached the wide scope of application that Babbage had envisioned. Even so, it is generally held, according to Spencer,[1] that Burroughs' design is the soundest (mechanically) ever conceived for the indented purpose.

Because Babbage's real contributions had been partially buried under an immature technology, men like Burroughs and Hollerith had to re-invent workable devices. Hollerith devised a scheme using a variation of Jacquard's cards to facilitate the tabulation of the 1890 census. His basic concept, using the holes in a particular card to activate a series of electrical counters, is still widely used wherever punched cards or tape appear. The general notion of calling such cards "IBM cards" is well-founded, since Hollerith later sold his interest to a predecessor of the International Business Machines Corporation.

The period just prior to World War II produced the first applications of electrocic technology to the computing function. Dr. George Stibitz directed several projects at the Bell Laboratories.

---

[1]Donald D. Spencer, Computers in Action: How Computers Work (Rochelle Park, N. J.: Hayden, 1974), p. 20.

Professor Howard Aiken of Harvard University directed the development of the Mark I, the first large-scale automatic calculating machine to be put in operation. Although primitive in comparison with today's integrated circuit machines, the Mark I was both versatile and accurate.

The usefulness of the Mark I and other developments in the analysis of wartime situations provided additional impetus to further the computing science. Dr. John von Newmann conceived a computer utilizing the binary system for internal data handling and the idea of a stored program of operations. The revolutionary and prophetic nature of such proposals is likened by Spencer[1] to someone's submitting plans for a Boeing 747 shortly after the Wright Brothers' flights in 1903.

The computers built on the ideas and under the direction of Dr. Stibitz, Professor Aiken, and Dr. von Newmann utilized current technology; that is, vacuum tubes and relays were used as storage and operational devices. These were necessarily large, cumbersome, slow, and heat-producing. A major breakthrough, important to all phases of the electronic industry, was the development in 1947 of the point-contact transistor by Messrs. Schockley, Bardeen, and Brattain of the Bell Laboratories, and the subsequent development by the same men of the junction transistor in 1948. The reduced size and power requirements

---

[1] Ibid., p. 26.

of this new device have led to extreme miniaturization, as witnessed by the processes of medium- and large-scale integration. By these processes, numerous transistors and associated components are fabricated by chemical means on small chips of a semi-conducting material such as silicon. The physical proximity is such that very little elapses while electrical currents travel between components. In addition, the time required for a transistor to change states, "on" to "off" or back, is so brief that times on the order of a few nanoseconds are now typical (one nanosecond = 1×10^{-9} second, the time required for light to travel a distance of 29.978 centimeters or approximately 11.80 inches; recall that light travels approximately 2.99776×10^{10} centimeters per second or 186,272 miles per second[1]). This transition time enables incredible speeds of calculation, storage, retrieval, and manipulation, with relatively small physical size and minimal power requirements. Were it to be built with vacuum tubes and relays, a computer with the proposed capabilities of the IBM 370 series would require a large building for housing, more electricity than a small town, and would be slower than today's pocket calculator in the hands of an experienced operator. As it is, this very powerful multi-purpose computer can be housed in a moderately-sized room, and draws no more current than a large air-conditioning system.

---

[1]Chemical Rubber Company, Handbook of Chemistry and Physics (Cleveland: Chemical Rubber Company, 1956), p. 13.

After about 1964, most accomplishments and developments in the computer field are found to be improvements, modifications, or refinements of earlier discoveries. Improvements in speed, accuracy, adaptability, and compactness have allowed the advent of the "minicomputer," a physically small computer with storage capacity less than fifty megabytes, usually costing less than $50,000. By way of contrast, an XDS Sigma/9 or IBM 370/195 rents for $35,000 to $270,000 per month.

Of all the phenomena associated with computers, perhaps the most remarkable is the brevity of time associated with their development. The first mechanical aid to computation, the abacus, is traceable to approximately 3000 B.C. The next major advancements in usable devices came after 4500 years, in the seventeenth century, with Napier's Bones and Oughtred's slide rule. The abundance of mechanical gadgets developed over the next three hundred years is related to other mechanical improvements pursuant to the abacus and Napier's Bones. Among these developments were the first mechanical calculating machine (Pascal); the first use of punched paper for mechanism control (Bouchon); the first mechanism totally controlled by punched "program" cards (Jacquard); the first machine conceived in a form that could now be called a "computer" (Babbage); the first usage of punched cards for processing numerical data (Hollerith). Beginning with Shannon (who proposed the application of Boolean algebra to switching circuits), the Mark I (the first electro-mechanical computer put in operation),

and the ENIAC (the first electronic computer put in operation), the development of computational devices left the strictly mechanical realm and entered the electro-mechanical world. The incredible sophistication, reduction in size, and versatility of the computers of the 1970's are all due to advancements made since ENIAC (1946). The staggering amount of technology developed and uses found in these thirty years far outstrip the total accomplishments in the field of computational devices over the past five thousand years.[1] The impact of the rapid advance on society is difficult to comprehend; the person educated before the 1950's has had to learn new approaches to computation, and the present generation has demanded worthy and varied use of a technological tool unknown to its forebears. For the young person of the 1970's, learning about computers requires little more than finding one and receiving instruction in its use, whereas that person's parents would have been hard-pressed to find one, much less to seek instruction in its application. The prospect of what the next thirty years will bring is staggering to the imagination.

The notion of mechanizing computation both has helped to generate, and has been helped by, the conception of technological advances. Most men have difficulty utilizing available materials and technology

---

[1]A schematic representation of some of the events named and the time element involved is given in figure 1 (a.v.).

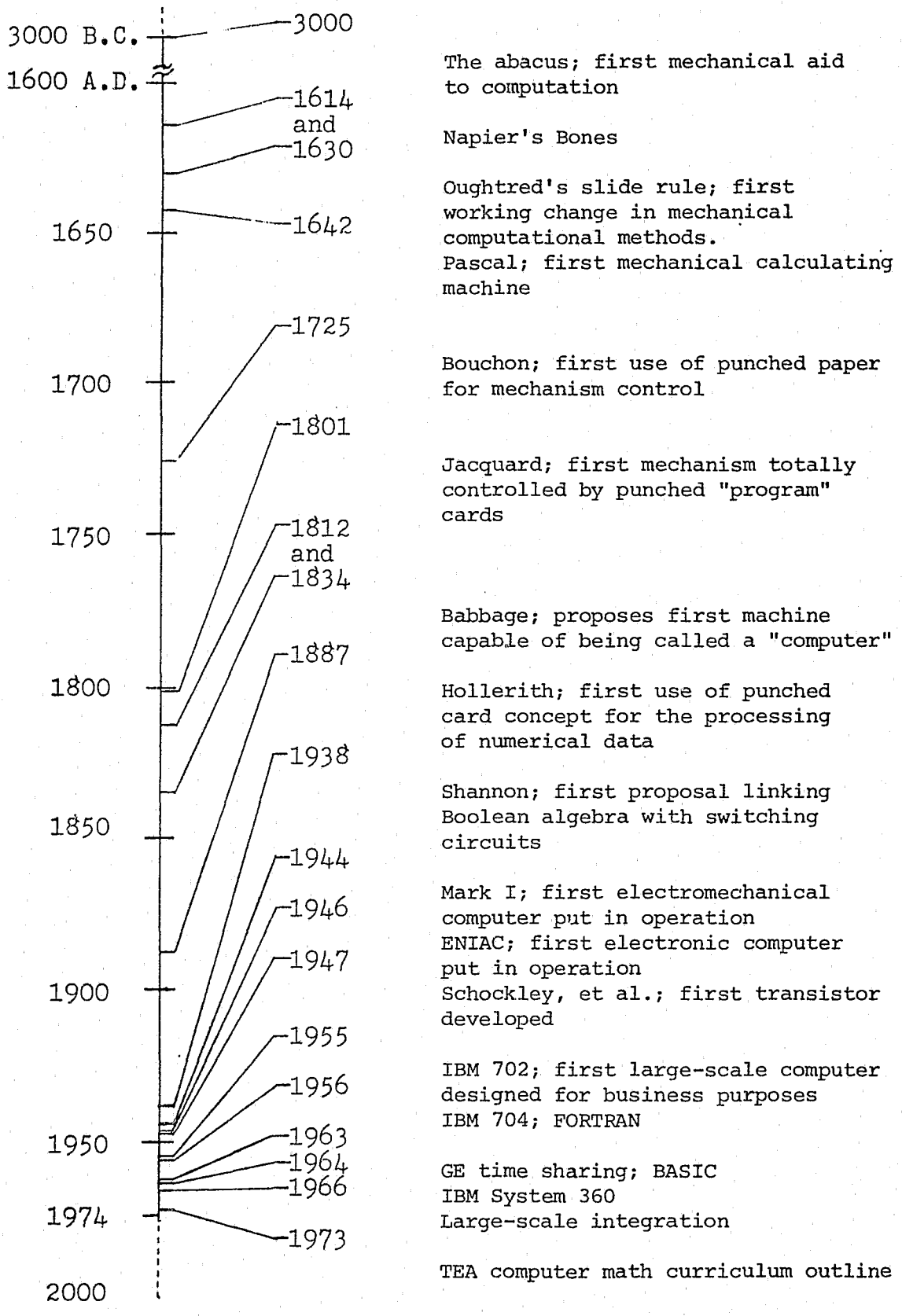


Fig. 1. A Schematic Representation of Some Important Events

to their maximum; a few, like Babbage and von Neumann, must wait to see technology allow full usage of their ideas.

The Nature and Structure of Typical Analog and Digital Computers

The modern computer falls into one of two rather broad categories, digital and analog. The digital computer uses and furnishes data that is in discrete units--a sum of money, solutions to an algebraic equation, statistics based on sales data or educational processes, etc. On the other hand, the analog computer deals primarily with changing physical phenomena--rotation of a shaft, variation in gas pressure during a manufacturing process, shifting gravitational forces, movement of a gyrocompass as a missile traverses its trajectory, etc. Whereas the digital computer acts upon numbers and other such actual data, the analog computer acts upon data gaines from a model or "analog" of the real occurrence; this model usually takes the form of a varying voltage whose variations are symbolic of physical changes actually occurring elsewhere.

There have been significant developments in both types, but the most publicized advances are those dealing with digital computers. It should be noted, however, that the technological feats associated with the Apollo missions and other space projects have been made possible by computers utilizing both vast digital procedures and "real-time" analog analyses ("real-time" operation refers to the processing

of data rapidly enough to allow the results to affect the device or condition producing the data).

All computers have certain basic structural features in common; it is the varied approaches to each component which serve to make competition keen and productive. Figure 2 illustrates the five major components of a computer: the input medium, the storage unit or memory, the arithmetic unit, the output medium, and the control unit.

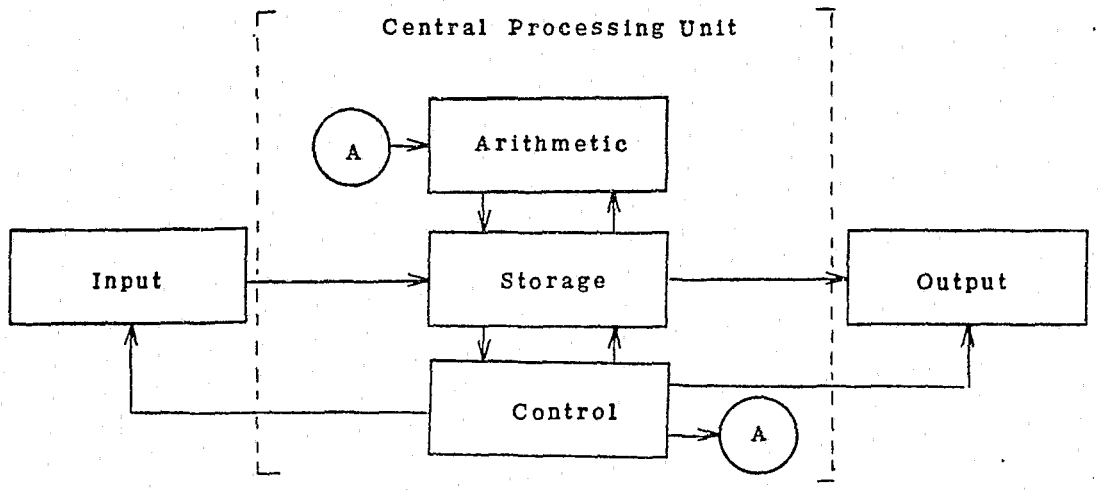


Fig. 2. Schematic Chart of Computer Functions

It is through the input medium that the program, or sequence of operations, is entered into the computer, along with the data which the program is to manipulate. The input for a particular unit may take any one of a variety of forms; in fact, the adaptability of the input device to the needs at hand often determines the effectiveness of the computation.

Certain forms of input are quite common for digital computers; one is the card reader, which senses holes punched in cards or marks placed

upon cards. The cards contain data or program instructions in a form easily handled both by operator and machine. The machine can read the cards rapidly (from fifty to over 1000 cards per minute), and the operator can re-order the cards, quickly replace an incorrect card with a correct one, or add or delete groups of cards with very little effort. The cards are read either electromechanically (using fine wires making electrical contact through the punched holes) or photoelectrically (either using lights coupled with light-sensitive devices, shining through the punched holes, or using such light sensitive devices to sense a reflective area on the card, placed by pencil to indicate a bit of data).

A similar unit is the punched tape reader. A long strip of paper, rolled for convenience, is perforated so as to contain certain information, such as data or program steps; this perforated tape is then passed through either a mechanical reader or a photoelectric reader. The photoelectric reader is very similar to the card reader. The mechanical tape reader is more complex: The tape is moved so that the next set of holes is directly over a set of small pins; after the tape comes to rest, the pins are pressed by springs against the paper. Where there are holes, the pins pass through them, allowing an electrical switch to close; where there are no holes, the pins are prevented from passing through and from allowing the switch to close. The pins are then retracted to their initial positions, and the tape is moved to the next position.

Another input medium common to digital computers is the keyboard. Available from various manufacturers in many styles and with many diverse features, the keyboard is a most useful input device; it provides a printed copy of information being presented to the computer in a form meaningful to the operator. On time-sharing systems--systems which allow several users to process programs apparently simultaneously--the keyboard is the principal means of input, as well as output. On batch-load systems--systems which usually use cards or tape as input and process only one program at a time--the keyboard and its printer provide a monitor for computer function and usage. It provides notices to the operator of malfunctions or conditions that are out of the ordinary; it also provides a convenient means for diagnosing a malfunction, for cards and tapes are not so readily used as are ordinary English or FORTRAN or other statements typed with the keyboard.

Occasionally, input takes the form of magnetic tapes; if a program or set of data has been developed elsewhere, perhaps on another computer, then a convenient method of transferring such information is by way of one or more reels of magnetic tape. The reader is a sophisticated version of the ordinary reel-to-reel recorder available for home or broadcast use; it is specially built to allow the tape to pass the reading heads at speeds up to 150 inches per second[1] (this compares with

---

[1]Matthew Mandl, Fundamentals of Electronic Computers: Digital and Analog (Englewood Cliffs, N. J.: Prentice-Hall, 1967), p. 167.

home recorder tape speeds of seven and one-half to fifteen inches per second). Such speeds allow handling in excess of 90,000 characters per second, with some units capable of handling 240,000 characters per second.[1]

Optical character readers are also being used for direct input. Characters printed in a special typeface can be read directly by photoelectric means, allowing the input to be usable as information both by the operator and the machine. Strides have been made toward recognition circuits capable of reading hand-written symbols. Carefully controlled character shapes are usable, but the general, randomly-shaped human handwriting is not yet within the reading capability of the ordinary character reader.

Once the desired program and data are inside the computer, they are stored temporarily in one of a variety of memory devices, to be recalled later as the program is executed. The same memory devices serve in other ways during the computing process.

One of the principal types of memory is the magnetic core memory. Small toroids or "doughnuts" of magnetic material called "cores" are woven, almost exclusively by hand, into a network of fine wires. The electronic circuits which control access to the memory are called "drivers"; by choosing the proper pair of wires that intersect paths at a

---

[1] Ibid., p. 173.

particular toroid or core, enough electrical current can be passed through the center of the core to change its magnetic state and thus to store or "write" one bit of information. Grouping these cores into large patterns allows many computer words, each with thirty-two bits, for example, to be stored at one time; one core is used for each one of the bits of information in each computer word. It should be noted that different computers use different lengths of words; the numbers vary from eight to as many as sixty bits per word; each word is simply a grouping of bits of information usable by the computer.

Reading information stored in a core memory is very similar to storing it; a current is passed through certain wires, and if the particular core was magnetized in the right way, the current causes the magnetic state to change back to its original state. This causes a current to flow in a third wire, called a "sense" wire, which then carries the information to the driver circuits for transfer back to the computer. Since this destroys the information stored in the core, the drivers must then re-write all the bits that were read back into the core memory. Such a memory has what is called a "destructive read-out," since reading information out of it destroys the information. The core memory is a versatile and reliable memory device, and access to stored information is very rapid. It is chiefly used for storing numbers being operated upon, for storing programs, or for use as an "electronic scratch-pad" during operation.

Several other types of memory devices use magnetic characteristics in their structure; instead of a core of material they make use of a thin film of material placed on some non-magnetic base. The three most common such devices are the magnetic drum, the magnetic disc, and the magnetic tape. The drum is rarely seen now in new computers, for the difficult manufacturing processes make it quite expensive. The drum consists of a cylinder coated with a thin film of magnetic material. Mounted around the periphery of the drum are numerous reading and writing devices called "heads"; the writing head causes a small magnetic field to pass through the drum's film and change the magnetic state of that particular spot. By placing enough of these heads along the drum, many circumferential tracks of spots can be used simultaneously.

As the drum revolves at a high rate of speed, the driver circuits keep track of the current location of each spot on the drum, and can call for the right information as it passes under the read head. The magnetic field in the film causes a small current to flow in the read head, and this is returned to the driver circuit to be used by the computer. The read and write heads must be mounted so close to the drum that any irregularities in the drum, in the film, or in the head alignment can cause the head to strike the drum and ruin it; it is this threat which demands such close and expensive manufacturing tolerances.

A more recent application of thin magnetic film is the magnetic disc. Shaped like a large, thick phonograph record, the disc rotates

between read/write heads at high speeds. The same read/write process is used as was used on the drum. Even though the basic idea of a rapidly moving magnetic surface is used, the disc is more efficient and more economical, because less physical space is required, less stringent manufacturing processes are involved, and less expensive materials can be used for the disc itself. In addition, several discs can be mounted in a stack, with heads mounted between them, to provide an even more compact arrangement. An additional feature is an interchangeable disc pack, allowing almost unlimited storage capacity. This allows programs using a particular language to be stored together or allows an expanded data or program library. Some smaller computer installations use an interchangeable single disc with the same results in versatility.

A variation in the disc described above has appeared: it is a flexible disc, made of a thin, but stable film of plastic coated with magnetic material. Instead of rotating with a small clearance between the disc and the heads, the flexible or "floppy" disc is pressed into direct contact with the heads, improving the efficiency of the reading and writing and greatly reducing the demands on manufacturing tolerances. These flexible discs can be quickly interchanged and easily stored. They can even be rolled and mailed, much as a drawing or chart might be.

The magnetic tape already mentioned as an input medium is also widely used as supplemental or "auxiliary" storage. Several characteristics especially qualify tape for this usage. A typical reel of tape

contains some 2,400 feet of tape and can store as much information as 400,000 punched cards.[1] Such reels are usually ten and one-half inches in diameter with large hubs. These reels of tape are primarily used for large amounts of data which need to be preserved, but which will probably be used in roughly the same sequence as it appears on the tape. The physical situation of a long piece of tape with information placed along its entire length requires that a definite, and sometimes long, time must elapse between the time that information is requested and the time that its location is found on the tape. Tape is thus referred to as a "sequential" or "serial" access medium, contrasted with a "random" access medium, such as the magnetic core memory.

Similar usage is made of the Phillips design of tape cassette, especially in small computers or minicomputers and in programmable calculators. The convenience of size and interchangeability makes the cassette a most attractive storage medium.

Experimentation and research are being conducted to find more efficient, more compact, more reliable, or more economical memory devices. Such techniques as semiconductor technology, cryogenics, plated wires, holography, direct optical storage, cathode ray tube storage, and others have had varying degrees of success. Out of these pursuits will surely come the technique for producing small, inexpensive computers for home and business.

---

[1]Spencer, p. 75.

After the data and program directions have been entered and properly stored, the computer must begin to process the data and perform specified operations on it. The unit which oversees the entire process from input through storage and operations to output is the computer control unit. This unit interprets the program commands and determines the sequence to be followed as data is processed from input to an appropriate output. Since the control unit cannot make rational choices, all possible conditions to be encountered must be planned for. The unit can then call on its limited, but adequate vocabulary to interpret commands, and if an unfamiliar command appears, it halts program execution.

One remarkable characteristic of control units is the capacity put there by the designer to keep accurate tally of all operations performed, to keep accurate accounts of the locations of all stored information, and in the case of a time-sharing system, to keep track of which user is being served and of where his data and programs are located. The actual mechanics of performing the tasks may be straightfoward, but the speed of operation is phenomenal.

Under the direction of the control unit, data is moved from input or memory to the arithmetic unit where all of the actual operations are performed. The repertoire of operations is relatively limited, including only the four arithmetic operations, numerical comparisons, and certain other algebraic functions. In most computers, the trigonometric

functions are performed with series arithmetic or other software procedures; the great speed with which this is accomplished keeps the extended process from significantly slowing the program execution.

The results of the program's manipulation of the data must ultimately be put into some form accessible to the operator, or perhaps to some other device or computer. The medium used is known as an output. For operator usage, a printed output is commonplace.

Several categories of printers are currently in use. The keyboard, already mentioned in connection with the input function, also serves well for limited use with many systems, but especially with time-sharing systems, where it is customary. The keyboard in its various forms is relatively slow in comparison with computational speeds.

Faster speeds are possible with the line printer, which uses various means to print several characters in one concerted effort. One of the most effective means used to accomplish this feat uses a metal cylinder engraved or molded so as to have all the alphabetic, numeric and special characters in every available printing column, placed in an order around the cylinder. As the cylinder revolves, a hammer placed in each printing column strikes the paper and ribbon against the proper character, whose position is sensed by the printing driver circuitry. Such a printer may be capable of printing more than 1000 lines per minute, each with up to 136 characters. Even at these

speeds, however, the printer may not produce output as fast as the computer provides the information.

Other output devices are specially tailored for specific requirements, such as the graphic plotter which can produce line drawings, lettering, and plots of algebraic or other functions. Cathode-ray tube displays are frequently used for output (and occasionally for input) for time-sharing systems; these can provide graphic or other data quickly, and results of alterations in programming can be seen rapidly. Occasionally, output is required in the form of paper tape or punched cards, and appropriate equipment is available to accomplish this. Other equipment designed to fill a particular need is used as the situation demands.

Although to this point the discussion of computer structure has been concerned with digital computers, many of the same structures are part of analog computers. The basic ideas behind the input, control, arithmetic and output units are very similar, with the differences being very important.

Input to an analog computer usually takes the form of some type of voltage variation. As a rule, several voltages are involved, and the computer investigates or controls the relationships of the inputs. By using devices called analog-to-digital converters, a continuously varying voltage can be converted into a signal with discrete changes roughly proportional to the shape of the original input. This conversion allows processing of the data for certain purposes by a digital computer.

The analog computer performs its most notable tasks as it applies logarithmic and other exponential processes to a signal input, or applies the differentiation or integration operations from calculus, tasks all but impossible for digital computers. By clever utilization of the circuit characteristics of capacitors, resistors, and operational amplifiers, the analog computer, through its own special type of control unit and "arithmetic" unit, can solve very complicated differential equations dealing with such topics as thermodynamics, transient electrical noises, and simultaneous motion of several objects. The problem of a spacecraft launching is particularly perplexing, for it involves the changing effect of gravity as the craft moves away from earth and closer to, say, the moon, while the craft itself changes in mass as it loses fuel and spent engines. This type of problem is readily solved by analog methods, with digital techniques handling the back-up in storage and data transfer.

Output from analog computation usually falls into two distinct categories--printed or graphic output, sometimes known as "hard copy," similar to digital output, and electrical information, used to control a process or device. Graphic output can take the form of plotting voltage (as it represents some quantity) against the passage of time on a continuously moving strip of paper, or plotting the simultaneous variation of two voltages on the same graph in x-y form. In such a plot, one voltage would control the horizontal or x motion of a pen,

while the other voltage would control the vertical or y motion of the pen.

The availability of electrical output allows "real-time" use for analog computers. The ability to operate in "real time" is generally understood to mean that the results of calculation and processing are available for control of the process or device being monitored. In this type of operation flight computers on the ground and on board spacecraft are able to control the flight path of the craft to permit a rendezvous or a re-entry with very little error or operator intervention. Similarly, manufacturing processes, such as chemical or petroleum, must be continuously monitored for pressures, content, and temperatures so that the result is predictable and within the prescribed limits.

A basic difference between digital and analog devices lies in the scope of application. Most digital computers are structured so as to be very general in application; the development of FORTRAN, BASIC and other languages is based on the widest possible scope of usage. In contrast, most analog computers are capable of solving a wide variety of problems, but are usually conceived with very specific problems in mind. A particular problem may require new circuitry or a new interconnection of existing circuitry, rather than a new program that might suffice for a digital computer use.

SELECTED CHRONOLOGY OF COMPUTER-RELATED EVENTS

ca. 3000 B.C.	"Suan Pan" (the Chinese abacus)
1614	John Napier ("Napier's Bones")
1630	William Oughtred (slide rule)
1642	Blaise Pascal (first mechanical calculating machine)
ca. 1690	Gottfried Leibnitz (improved mechanical calculator)
1725	Basile Bouchon (drawloom controlled by punched paper paper roll)
1728	M. Falcon (loom using punched cards)
1741	Jacques de Vaucanson (automatic loom using punched metal drum)
1801	Joseph Marie Jacquard (loom completely controlled by punched cards)
1812	Charles Babbage ("Difference Engine" conceived)
1834	Charles Babbage ("Analytical Engine" conceived)
1850	D. D. Parmalee (key driven adding machine)
1854	George Boole (published An Investigation of the Laws of Thought . . . in which the foundations of Boolean algebra were proposed)
1868	Christopher Latham Scholes Carlos Glidden Samuel W. Soulé (first practical "typewriter" patented)
1873	E. Remington & Sons (Remington No. 1, Remington's first calculator)
1875	Frank Stephen Baldwin (reversible four-process calculator)
1878	W. T. Odhner (calculator, "the Odhner wheel")
1879	James Ritty (cash register invented)
1884	William Seward Burroughs (first commercially practical adding-listing machine)

1884	John H. Patterson (commercially successful cash register; formed National Cash Register)
1885	Dorr Felt ("Comptometer")
1887	Leon Bollee (multiplication by direct machine methods, not repeated addition)
1887	Dr. Herman Hollerith (punched card tabulating machine, "Census Machine")
ca. 1900	Dr. Herman Hollerith (formed Tabulating Machine Company; later sold, became IBM)
1909	Charles F. Kettering (accounting machine, a teller machine for certifying passbooks)
1910	James Powers (punched card system, 240 keys)
1911	James Powers (formed Powers Tabulating Machine Company; later merged into Univac Division of Sperry Rand)
1911	Jay R. Monroe (first keyboard rotary machine to attain commercial success)
1914	Oscar and David Sundstrand (ten-key adding machine)
1920	James Smathers (electric typewriter developed)
1937	Howard Aiken (began work on Mark I at Harvard)
1938	Claude E. Shannon (thesis for M.S. at MIT proposing use of Boolean algebra concepts to analyze relay and switching circuits)
1938	Bell Telephone Laboratories (began work on electro-mechanical computers)
1940	Dr. George R. Stibitz (began work on "Complex Calculator")
1944	Mark I completed
1945	Dr. John von Neumann (recommended use of binary system internally; recommended "stored program" concept)
1946	ENIAC operational (first electronic digital computer; used parallel processing)

1947	IBM Selective Sequence Electronic Calculator completed
ca. 1947	IBM 603 electronic multiplier completed
1947	William B. Schockley Walter H. Brattain John Bardeen (developed point-contact transistor at Bell Labs)
1948	William B. Schochkley Walter H. Brattain John Bardeen (developed junction transistor at Bell Labs)
1949	EDSAC (first computer to incorporate von Neumann's ideas)
1951	Whirlwind (MIT; first "real-time" computer; used magnetic core memory)
1951	UNIVAC I installed at Census Bureau (utilized magnetic tape input)
1952	EDVAC (University of Pennsylvania; true stored program; binary program and data)
1952	IAS (Princeton; personally directed in construction by von Neumann; the direct forerunner of: ILLIAC, University of Illinois; JOHNIAC, Rand Corporation; MANIAC, Los Alamos; ORDVAC, University of Illinois; WEIZAC, Weizman Institute, Israel)
1952	William B. Schockley (field-effect transistor theory announced)
1953	George C. Dacey Ian M. Ross (field-effect transistor developed)
1953	IBM 701 delivered
1955	IBM 702 (first large-scale computer designed for business purposes)
1955	IBM 705 (made 702 obsolete before more than a few were installed)
1955	IBM 704 (gave IBM a near monopoly in large-scale scientific computer field)

1955	John Backus (developed FORTRAN for use in IBM 704)
ca. 1956	Dr. Grace Murray Hopper (developed FLOMATIC while at Eckert-Mauchly, forerunner of the Univac Division of Sperry Rand; FLOMATIC was later incorporated into COBOL)
1962	Stephen R. Hofstein Frederick P. Heiman (developed MOS transistor at RCA)
1963	John G. Kemeny Thomas E. Kurtz (developed BASIC at Dartmouth for use with a time-sharing system by General Electric)
1963	First time-sharing system implemented (GE)
1964	IBM System/360 announced (major change in philosophy, to reflect a comprehensive problem-solving ability; used integrated circuits with MOS transistors and FORTRAN IV)
1965	PDP-8 (Digital Equipment Corporation; brought widespread use of the "minicomputer")
1966	LINC-8 (DEC; another widely used minicomputer)
ca. 1966	Large-scale integration developed at several laboratories (enabled great reduction in size; also foreshadowed pocket calculator era)
1966	Sigma 2 (Scientific Data Systems, now Xerox Data Systems; forerunner of a large line of minicomputers)
1968	TI 980 (Texas Instruments; first of TI's entries in the minicomputer field; forerunner of their "4-pipe" devices)
1971	IBM 360/195 and 370/155 (last of the 360 series and first of the new 370 series)
1971	IBM System/3 (IBM's entry into the moderate-size minicomputer field)
1973	IBM 370/195 (largest and most powerful of the 370 series)

SUGGESTED SOURCES FOR ADDITIONAL MATERIAL

Estes, James W., and Estes, B. Robert. Elements of Computer Science. San Francisco: Canfield Press, 1973. Especially note chap. 10, "Reflections on Computer Technology."

Mandl, Matthew. Fundamentals of Electronic Computers: Digital and Analog. Englewood Cliffs, N. J.: Prentice-Hall, 1967. Especially chap. 1.

Rothman, Stanley, and Mosmann, Charles. Computers and Society. Chicago: Science Research Associates, 1972. Especially note chaps. 2, 3, and 4.

Spencer, Donald D. Computers in Action: How Computers Work. Rochelle Park, N. J.: Hayden, 1974. Especially note chap. 2

_____. Computers in Society: The Wheres, Whys, and Hows of Computer Use. Rochelle Park, N. J.: Hayden, 1974. Especially note chap. 1.

Weiss, Eric A., ed. Computer Usage: Fundamentals. New York: McGraw-Hill, 1969. Especially note chaps. 1, 2, and 3.

COMPUTERS IN LAW ENFORCEMENT*

Why Use Computers in Law Enforcement?

The use of computers by law enforcement agencies and criminal justice departments is a relatively new innovation. There exists at the present time only a few systems utilizing computers, computer peripherals, and quasi-computer equipment. More and more law enforcement agencies are turning to computers for help in solving the many and varied problems facing these agencies.

The process of gathering, interpreting, and disseminating information is an important and time consuming operation of law enforcement agencies. Computers and computer systems have shown their effectiveness in carrying out these processes in other areas, and the systems that are now operating to assist the law enforcement community are showing that the performance capabilities of computer systems can greatly enhance this community's efforts. Increasing the efficiency of processing emergency calls, more efficient utilization of man power, improved accuracy in reporting, greater return on the investment of tax dollars, more meaningful reports for management, and the delivery of timely and more complete information to dispatchers and field personnel are some examples, and arguments for implementing computer systems to augment law enforcement efforts.

From utilizing the data processing capability of a computer, to developing its telecommunication and programming capability, law enforcement agencies are tapping every advantage a computer system can offer. In doing so, these agencies are able to serve the public in a manner that was previously impossible.

*Reports submitted by Mr. Jess Burris and Ms. Elaine Hardesty to Dr. J. L. Poirot, Math 3308 Class, Southwest Texas State University. 1974.

An Example of Information Processing, Storage, and Dissemination

The National Criminal Justice Reference Service (4), offers a wide range of information services to the nation's law enforcement and criminal justice community. This service provides information on research literature significant to criminal justice, distributes publications, answers inquiries, makes referrals, sends out listings of documents and announcements, and has established a clearing house for information on the energy crisis as it affects the criminal justice system.

The basic information source is a computerized data base of almost 10,000 documents. Material in the data base includes bibliographic information, descriptive abstracts, and is indexed according to established criminal justice terminology. Hard copies of all items in the data base are maintained for reference purposes, and many are available for distribution.

Having begun operations in 1972, nearly 19,000 registered users now avail themselves of this service. Any individual or agency involved, or interested in law enforcement may become a registered user by filling out an interest profile. A comprehensive list on over seventy-five subjects, ranging from alcoholism to rehabilitation is available for determining an interest profile.

This service began international operations in 1973. As the first such Federal system in the field, the National Criminal Justice Reference Service stands as an example for topic information storage. Without this system large amounts of data would exist in numerous locations, and be obscure to the most diligent researcher.

Existing Systems and Their Operations

A) Huntington Beach, California's "Command and Control" system, developed by Motorola, was the first computer-aided system in the nation. The nerve center of the system is the computer and CRT Video Display Terminals. The individual officers in the field are equipped with the Motorola MODAT mobile digital communications system, linked to his Motorola MICOR mobile two-way radio or the HT-220 HANDIE-TALKIE two-way portable radio. The Motorola teleprinter furnishes the patrol units with a permanent and instant hard copy of all communications. The Motorola Insta-Call communications recorder provides for immediate rechecking of any complainant's call if there is any doubt as to its content. Located in the police department's communication center is a Microfiche display screen which is capable of calling up more than 75,000 different map negatives. The total system is geared to city-wide usage through Digital 11/15 computers, and master reports are furnished through a Burroughs' computer.

When a complaint is called in, the computerized Command and Control System allows the complaints officer to receive the call, which is simultaneously registered on his and the dispatcher's CRT Video Display Terminals. The display itself includes the time and date (registered automatically), and the complaint officer adds the complainant's name, address of the incident, and nature of the incident. The dispatcher is also equipped with another CRT unit which presents him with the status of every police officer in the field. This status information includes - available, en route, at the scene, on investigation, or at station, and is controlled by the mobile units.

When the dispatcher makes his determination on assignment, he activates the system both verbally and electronically. As he is telling the field officer of the assignment, he activates the mobile teleprinter, which provides a foolproof backup. This hard copy of all communications both reduces time in copying assignments and errors or repeating of messages.

Silent burglar alarms are directly connected to the system. In the event that one is triggered, the computer automatically selects and notifies the patrol unit in that particular location that can respond the fastest. This feature eliminates the time that would be required by the complaint officer and dispatcher, allowing for faster response time in emergency situations.

The Huntington Beach system can also access the California Law Enforcement Teletype Service, and is utilized by both the Fire Department and Harbor Patrol. All agencies agree that the system is providing faster response time in emergency situations, greater accuracy of communication, superior utilization of manpower, and a much more efficient return on the investment in tax dollars (5).

The time element has been greatly reduced through computer usage, but another feature is the compilation of data, providing management with information for planning and better decision making. The data management system is a facet which is saving many man hours in the compilation of reports such as those which the department sends to the FBI and Uniform Crime Reports. A special 80 character line, programmed for input at the CRT's and accompanying every complaint entry, provides for coded information concerning the disposition of every case. This information is used, along with the original entries, to provide the department with operational

management and modus operandi systems. Among the data which is compiled daily within the system for future evaluation and use are original data elements such as daily case numbers, date and time of entries, time of dispatch, time of officer response, arrival and clearance, time of disposition, list of officers assigned, address of incident, response district, area or police beat number, responding agency, initial classification, and priority and file retention identification.

B) The New York City Police Department's Communications Division's SPRINT, Special Police Radio Inquiry Network, is a computer (2) assisted dispatch system geared to fast and efficient processing of public complaints. Around the clock, every day of the year, it's 62 emergency operators - including four Spanish-speaking - receive more than 19,000 requests for assistance and inquiries from the public. Part of its critical responsibility is the job of relaying an average of 1,100 reports of fire to the Fire Department, and hundreds of calls for ambulances. In 1973, Communications Division's police radio dispatchers transmitted two-and-one-half million radio runs to police officers on patrol. Transmitting via UHF and VHF radio frequencies, Communications Division (CD) messages link radio motor patrol units, detective cruisers, Emergency Service rescue squads, and aviation units. The present number of broadcasts is a reduction of 15% from pre-SPRINT days. This has been accomplished through screening, i.e. referring non-emergency calls to local precincts and non-police matters to other appropriate city, state, and federal agencies.

The system utilizes two IBM 360 computers and telecommunications hardware to keep the entire system from bogging down under the massive volume of calls for police assistance. CD is arranged into five area radio

rooms corresponding to the city's boroughs. Each area has its own battery of dispatchers and emergency operators, called turret operators. Incoming calls are intercepted by an automatic call distributor (ACD). This device identifies the borough the caller is dialing from and automatically channels the call to the appropriate turret operator servicing that area. The ACD polls each operator's position until it locates one which isn't already servicing a call. During peak periods, overflow is directed to additional turret operators or to those concerned with other boroughs that are idle. Each turret operator and dispatcher has the capability of accessing adjoining zones, thereby allowing for a coordinated effort between many zones directed by a single dispatcher.

After receiving a call, the turret operator, by using a combination of coded messages and regularly spelled out words, feeds the caller's name, nature of the complaint, address and incidental details into the computer through his CRT Video Display Terminal. The total incident display presents the turret operator with all the relative information, including the turret operator's identification number, date and time the message was received, and its numerical order among all the calls received during the 24 hour period. After recording all the information the turret operator keys the SPRINT system and the computer analyzes the information, searching for errors. A report bearing a nonexistent address for example will be rejected due to the pre-programming of all valid addresses within the city.

Several means are available to the turret operator to overcome filing misinformation into the computer. First, all messages received are recorded twice. Five master tapes, 40 recording tracks on each, constantly revolve in a secured tape room within the center, auditing every conversation.

A second recording device, called a message repeater, is affixed to the turret operator's desk and wired directly into his CRT. This repeater can record a full three hours of conversations, between complainants, radio dispatchers, and patrol units. This feature allows for playback of a complaint in the event that a caller floods the operator with hasty information and hangs up. This repeater obviates the need to disturb the master tape; no interruptions occur and no cumbersome cross-filing system is necessary.

The SPRINT computer is also programmed to preclude human error. Built into the system are special alias, place name, and misspelling files. The former category consists of an extensive cross-reference of streets, major traffic arteries, and intersections which have more than one name or designation, or were once known by another name. The place name file lists 13 categories of places such as schools, hospitals, hotels, theaters, and parks. The misspelling file contains thousands of commonly misspelled names of streets, which means that the computer will scan this file before rejecting a location as being nonexistent.

When the computer accepts the total display information, it determines the precinct of occurrence, the appropriate patrol car to service the call, and alternate units available for response. A summary, one-line coded message is then presented on the dispatcher's display screen. Up to ten individual incidents can be viewed at one time, and during peak periods the terminal can be keyed to allow a dispatcher to view up to 99 incidents. The dispatcher assigns priorities according to the nature of the incidents, and then broadcasts them to the computer selected patrol unit. Once assigned, he keys his monitor, which brings up the more in-depth Total Incident Display. From it he can relate to the investigating officers all the details of the

complaint as reported, and any additional information the computer was able to analyze pertinent to the original information. Precinct sector maps displayed on a lighted viewing screen permit dispatchers to assist field units in the investigation of complaints. Detailed on them are addresses within each precinct sector, diagrams of buildings' lines, and the location of alleyways and yards not visible to the investigating officer from the street. Once an assignment is given to a patrol unit, the computer sets a prescribed amount of time for its completion. If a disposition is not returned within the allotted time, the computer automatically generates an overdue signal, upon which the dispatcher can act.

The Central Complaint Desk Unit continually receives computer printout sheets listing, by precinct, all reported crimes transmitted by radio dispatchers. Throughout the day, each station house is required to supply the complaint desk with the precinct complaint number identifying the investigating officer's reports. That information is recorded and filed for reference. Statistical reports are generated from the various information entered into the data base, come compiled on a daily basis (1). Some examples of reports are: Hourly job distribution list - weekly report indicating the work load performed by each precinct unit, and the average time each unit requires to service a call; Workload summary - weekly report by day and tour, listing total number of jobs occurring within a sector, the number of jobs each patrol unit processed inside/outside its sector, and also makes a comparison with the previous week's statistics; Monthly Personnel Evaluation Report - measures performance of CD workers, number of hours worked, whether as turret operator or dispatcher, their error percentage, and this report is used for training purposes.

The SPRINT system is connected to a teletype network that can access the Mayor's office, JFK and La Guardia airports, the police commissioner's office, and the Transit police. Programmed into the computer are listings of stolen vehicles, impounded vehicles, stolen merchandise, and warrants for wanted individuals. Future plans include accessing the National Crime Information Center at FBI headquarters. The second IBM 360 computer, the capacity of which is being studied and evaluated, is expected to augment SPRINT with terminals installed in each precinct station. As the system stands, it is increasing the efficiency of processing emergency calls, while decreasing police response time. It is also providing management and field personnel with invaluable information, from which more efficient allocation of police resources can be realized.

C) At the district level, Queens County, one of the five boroughs comprising New York City, is equipped with a Miraquic identification and coding system. This system was designed to decentralize certain criminal records. Based on the discovery (8) that most criminals are recidivists, and tend to restrict their activities to a limited geographic area, this system was inaugurated in March of 1973.

Miraquic (Kodak Miracode II Queens Identification and Coding) utilizes microfilm equipment to record mug shots and arrest information, and a viewing screen system which can access the microfilm files according to a coding system. Two separate banks of records are maintained; a record being the related information concerning a criminal. One file bank contains fingerprints, the other contains photos and arrest records. The information is recorded directly on microfilm, and stored in 16mm cassettes,

each of which can contain 600 records. Dividing the system into two files reduces search time.

The photo and arrest record file consists of a laminated card, one side contains the prisoner's mug shot - side and front view, while the other side contains the previous arrest information reduced in size. By coding in information the bank can be searched electronically very rapidly for specific descriptions. Twenty-five different categories are used for coding, including precinct of arrest, sex, race, vehicle, organized crime, alias, M.O., build, scars, tattoos, etc. By noting one or more descriptors, a victim can be presented on the viewing screen with all known offenders possessing that or those characteristics. Before this systems inauguration, a victim would have to go to the main headquarters in Manhattan and look through volumes of mug shots, many of which were not even close to the description of the offender.

The fingerprint file contains sets of fingerprints. Each single fingerprint is assigned a three digit number based on the pattern, the count or tracing and the core. With this coding system it is possible to search the files with only one or partial print; a feature not present in previous methods.

The Miraquic system, although it does allow for random search of the respective files, is not computer controlled. Systems that utilize a computer are much more expensive, which is a problem when considering the large number of units that would be required at district levels. This system is also much more reliable, not requiring the maintainance or subject to memory loss in the event of failure.

CONTINUED

1 OF 2

D) The police in Oakland, California use a high-speed digitalized computer system that borrows heavily from data handling technology developed in recent years for the U.S. armed forces. Key parts of the squad cars' systems are a terminal, a keyboard the size of a portable typewriter, a radio transmitter, and an electronic city map. At police headquarters, they have a small computer, another keyboard, terminal, and a large screen map. To run a check on a license plate, a policeman needs only to key in the letters and numbers of the license plate into the keyboard which is mounted on the transmission hump before the cruiser's front seat. Each letter and numeral is converted to binary code and radioed back to headquarters. The computer passes the request to PIN, the Police Information Network, which is a computer facility serving nine counties in the San Francisco area. In from 6-60 seconds, the information is transmitted back to the video-screen in the patrolman's terminal. Information provided includes the 1974 tag number; the year, make and model of the car registered for that tag; the registered owner's name and address; any warrants outstanding against the owner; and the fact of the car's theft if it was reported stolen. If the car is from some other part of California or out-of-state, the patrolman can check the license with the FBI's NCIC by punching in other buttons on the keyboard.

E) Glendale, California has also developed a computer based management information system for its police. Its computer operates with real-time data by receiving and storing data concerning requests for assistance as an accident occurs. Its system provides route dispatching of cars through the computer. When a citizen calls for assistance, the computer gets the telephone message that is typed in by the officer taking the call, selects the car most appropriate, and transmits the dispatch message on a mobile

output device.

Some police cars are equipped with an electronic map fixed to the dashboard. The patrolman simply inserts into the frame the street map of the area he is working and touches his finger to the nearest intersection. The pressure-sensitive back of the map holder determines the coordinates of the position, converts it to binary, and transmits this information back to headquarters. With this device, dispatchers can tell at a glance where the cars are, determine when a car is inappropriately out of service, and also permit tactical maneuvers with a number of cars, such as blocking of escape routes.

F) Tampa, Florida police use computer prepared exception reports to curb crime by selectively deploring its force to city areas where the incidence of crime deviates from the norm. The system works by dividing the city into a network of 200 grids. The size and shape of a grid is determined by natural boundaries, crime frequency, and population density. After analyzing various statistical inputs for robbery, burglary, and other crimes, their computer prints out a map of the city, showing the sections of the city where crime is on the rise. Monthly reports are now printed out, but weekly and daily reports are also available. These same techniques are applied to traffic safety. As a result, the city showed a 6.9% decrease in crime after using exception reports for a year, which is more than any other city its size in the nation.[1]

---

[1]"Computerized Police Assignments," American City, Vol. 86 (March, 1971), p. 18.

G) Police in Illinois use microfilming procedures to publish its "wheel book."[2] The wheel book consists of over five million vehicle registrations and is used for registration checks, tracing delinquent parking ticket violations, and in the driver's license administration. Before microfilming, it included 147 books and now it is a 48 ounce packet of 4x6 cards known as microfiche. A card is put into a TV-like viewer which is supplied by the state to 800 law enforcement agencies. Then the Computer Output Microfilming, or COM, converts the data into a readable form on microfilm. It can be connected directly to the computer for on-line operations or the magnetic tape units for later use. Paper facsimiles of any document can also be supplied in seconds. It takes less than ten seconds to search the book and new material can be added on at any time. Random searches can also be made when only the date or time of day is known relating to a particular request.

H) A police computer in Indianapolis, Indiana retrieves names from its files on a sound-alike basis when correct spellings are not known or when spelling errors are made on records.

Traffic Control

Most American cities will sooner or later computerize the control of street lights. When traffic control was computerized in New York in 1969, the rush hour accident rate was halved, there was a 70% reduction in the number of stops, and there was a 35% reduction in driving time.[3] New York's

---

[2]"Illinois Microfilms its 'Wheel Book,'" American City, Vol. 86 (April, 1971), p. 73.

[3]Stephen Solomon, "Now Computers Guide You Through Traffic Snarls," Popular Science, Vol. 198 (January, 1971), p. 56.

Traffic Commissioner, Theodore Karagheuzoff, says "Making more traffic move faster is not the principal object of this system. This purpose is to enable traffic to move more efficiently so that our streets can make their maximum contribution to the transportation of people and goods."[4]

Other benefits seen from computerized traffic control include: a less expensive alternative to street widening, reduced air pollution because of more efficient operations, and a reduced accident because of fewer stops and less driver irritation, and a historical data base for analysis of future transportation needs, reduced operating costs for motorists, and reduced street maintenance.

In the most sophisticated systems, cars are detected either by overhead ultrasonic devices or inductive loops buried in the pavement. Ultrasonic sensors are often chosen over those buried in the streets because the streets are torn up so often. The transducer portion of the sensor beams an ultrasonic wave at the highway. The solid-state receiver, mounted in a weatherproof cabinet on a pole, develops an output signal only when the reflective time is altered by a passing car. The sensors are checked about 60 times per second. Magnetic loops are also used for the detection of traffic. Frequency shift keyed-tone terminals feed the data from the loop detectors and controllers to the computer. The data received is transmitted to a central control office over telephone lines. Pulses sent by wires to the control center are translated into traffic density, volume, and speed data. Most systems use software packages and rely on historical analysis of traffic. The computer compares the traffic pattern to a

---

[4]Ibid., p. 55.

pre-stored pattern in memory to see which one it most resembles, and then selects and operates a corresponding control pattern. It overrides the last program sent by the computer. The computer provides all the system logic and timing required.

Los Angeles has a system that figures out new signal patterns as it controls traffic. While one part runs the current pattern, another part uses new data to run series of simulations until it finds a pattern that cuts the predicted "delay time" to a minimum. A signal pattern is based on three variables: "cycle time," or the interval from one green light to the next; "split," which is the ratio of green to red time; and "offset," the interval between a green light at one intersection and a green light at the next.[5]

Some studies suggest there are really only about twenty really different weekday traffic patterns, although IBM offers a package of 500 signal patterns. One doesn't want to work with too many patterns because a change takes from 8-15 minutes for the period of transition.[6] New York doesn't make a change more than once an hour.

A keyboard input/output console allows the traffic engineer to take control of an individual intersection and make timing adjustments for unforeseen circumstances such as an accident, weather, or holidays. There is also a fire pre-empt button to give the right-of-way to emergency vehicles and also a remote police panel that allows the police to adjust the machine status during nonworking hours.

---

[5]"Electronic Traffic Cops Take on Bigger Jobs," Business Week, No. 2184 (July 10, 1971), p. 58.

[6]Solomon, op. cit., p. 58.

The system also includes a secondary or fall-back operation where it reverts to local equipment in case of failures. Otherwise the system operates 24 hours a day, 7 days a week, and 75% of the time without an operator.

An electronically controlled display map provides real time data as to the state of each signal and indicates the presence or absence of traffic in various areas. There is also automatic reporting systems available that print hard copy reports indicating the status of equipment, and also includes timing, volume, and speed data.

Traffic control systems are costly. In New York, it costs about $2000 per intersection.[7] A federal program called TOPICS, or Traffic Operations to Increase Capacity and Safety, it supported by the Highway Trust Fund. The federal government usually pays 50% for a state-approved TOPICS program. SIGOP stands for Signal Optimization Program and is a cooperative project between the Federal Highway Administration and six selected cities--Kansas City, Cincinnati, Indianapolis, Seattle, Miami, and San Antonio. The cities pick the streets to be computerized and collect data on the traffic. FHA then furnishes the SIGOP tape. No funds are provided, but the only cost is staff time because no new equipment is needed.

Los Angeles also developed a computer system with sensors buried in the highways to cover 42 freeway miles. In addition to traffic guidance, it also controls on and off ramp traffic with lights, lights up electronic signs along the freeway to inform motorists of traffic problems ahead, and

---

[7]"Electronic Traffic Cops," op. cit., p. 25.

lights up signs telling motorists to tune in to local radio stations.

A Computer System Proposed for Great Britain (3)

At an Interpol Symposium on the use of computers by the police, held in Paris in 1965, delegates spoke of their countries' plans for using modern data processing equipment in the fight against crime. The British, in 1967, announced their plans for a Police National Computer Project. This proposed network would allow any constable who stops a car, e.g., to use his personal two-way radio to contact the information room, and the private teleprinter network from there to the computer, to find out in about 60 seconds whether the car is stolen, the occupants are wanted by the police, whether the driver has been disqualified from driving, or if any distinctive property in the car has been notified as stolen. The cost of this proposed system was estimated to be around 16 million pounds, and the system was expected to be operational by 1974.

Conclusion

Computers have shown to be an effective tool in the preparation and deliverance of meaningful management data for the leadership of law enforcement agencies at all levels. The data management systems alone may prove to be the most important breakthrough (5). This facet alone accounts for saving years of man hours in the preparation of reports. Statistics, that before were either nonexistent or late in compilation, are providing leaders with daily information upon which they may bases their decisions.

The systems now in operation are freeing more police officers for field duty, at a more efficient level of performance. Through the computers' multiprogramming capability, more calls are being handled faster and with

greater accuracy, saving valuable time. This feature places police officers at the scene of an emergency situation faster than ever before, and provides him with assistance in efficiently and effectively handling these situations.

The taping capability of computerized systems allows dispatchers to recheck information, and these tapes also are proving invaluable in the courtroom (1). The district attorney is able to describe events in detailed chronological order, giving precise times and locations, thanks to the programming of these computer systems.

The telecommunications capability, and real time operating of these computerized systems is another invaluable aspect. Other departments, such as fire departments, and teletype services, may be linked to the systems, allowing for superior efficiency in the handling of emergency situations. Coordinated efforts may be carried out easily and smoothly, thanks to dispatchers possessing terminals that allow for multi-call and inter-zone handling.

The efficient and effective utilization of computer systems presently in operation points the way for others to follow. The State of Texas for example, is planning a study to investigate the possibilities of computerizing some of the state's city police departments. With computer equipment becoming more economical and compact, it seems inevitable that one day the entire nation will be linked together, one system accessing another, in the fight against crime, and in the effort to better handle emergency situations.

BIBLIOGRAPHY

1. Sprint; Police Department, City of New York, PIB 72.

2. New York City Police Department Communication Divison; NYPD Printing Section.

3. Computers and Professional Criminals in Great Britain; Computers and People, Vol. 23, no. 7, July 1974.

4. A Comprehensive Reference Service Few People Know About: Law & Order, Vol. 22, no. 10, October 1974.

5. A Command and Control System; Law & Order, Vol. 22, no. 5, May 1974.

6. NYPD - From: Commanding Officer, Miraquic Project
   To: Chief of Detectivies
   Subject: Report of Miraquic Project for 1973; Feb. 20, 1974.

7. Miraquic, Illustrations, Index.

8. Miraquic.

9. Miraquic; Police News of New York, page 29, October, 1974.

10. Bauer, Chief E. O., Morel, Mayor Emery B., "Turn Police Files Into Information Centers," American City, Vol. 86 (May, 1971), p. 14-16.

11. "Computer Aids Police Management," American City, Vol. 87 (February, 1972), p. 27-30.

12. "Computerized Police Assignments," American City, Vol. 86 (March, 1971), p. 16-19.

13. "Computerized Police Communications," American City, Vol. 86 (May, 1971), p. 32-33.

14. "Computerized Signal Settings Speed Traffic Flow," American City, Vol. 86 (April, 1971), p. 27-31.

15. "Computers for Cops," Newsweek, Vol. 79 (June 5, 1971), p. 71-74.

16. Deweese, J. Taylor, "Giving the Computer a Conscience," Harper's Magazine, Vol. 247 (November, 1973), p. 14-18.

17. "Electronic Traffic Cops Take on Bigger Jobs," Business Week, No. 2184 (July 10, 1971), p. 45-46.

18. Fuller, F. J., Hernstein, H. I., Yagoda, H. N., "Computerized Traffic Control," American City, Vol. 86 (October, 1971), p. 109-111.

19. "Illinois Microfilms its 'Wheel Book,'" American City, Vol. 86 (April, 1971), p. 73-75.

20. Solomon, Stephen, "Now Computers Guide You Through Traffic Snarls," Popular Science, Vol. 198 (January, 1971), p. 86-90.

21. Venable, Clinton A., "Low Cost Computer Halves Driving Time," American City, Vol. 86 (March, 1971), p. 95-99.

22. Webb, Lee, "Computerized Police Systems in the US?," Current, Vol. 132 (March, 1971), p. 14-19.

23. Wilkins, Roger, "The Threat of Law Enforcement Technology," Current, Vol. 139 (October, 1971), p. 16-23.

COMPUTER DATA STORAGE

(An Example)

One of the crime analyst's biggest jobs is the organization of data for analysis. The electronic computer may be of most use to the analyst as a data storage and retrieval system. By use of the speed at which data can be recovered from the storage devices and by using the programming languages of the computer to soft information prior to print out, the analyst can save many hours of "clerical" work and concentrate on analysis and interpretation.

Figure 1 is an example of how a computer can "converse" for input of data on a burglary. The information typed by the person entering data is underlined. Keep in mind that a computer programmer is responsible for the conversation. We do not want to tive the impression that the computer is really "talking." Notice how easy it is to enter a report to the computer's file. In practice, a simplified code similar to those previously discussed, would most probably be used in order to speed up the data entry.

Figure 2 shows how a computer can sort information out of a file, based upon input from the analyst. Again the entry is conversational and easily understood.

```
BASIC
GO:
OLD OR NEW FILE:      POL←←OLD
FILE NAME: POLICE
FILE IDENTIFIER OR "RESTART": 7928
 COPIED FILE   POLICE
READY
READPF 4016 POLFILE
 COPIED FILE   POLFILE
READY
RUN
POLICE RECORDS:  VERSION 041775
PLEASE ENTER THE CODE TO ACCESS THIS PROGRAM.      114
DO YOU WISH TO ADD A RECORD? Y
POLICE RECORDS:  INSERTING!
INTO WHICH DISTRICT DO YOU WISH TO INSERT THE RECORD (1-8)? 4
INSERTING INTO DISTRICT  4 .
PLEASE ENTER THE TYPE OF RESIDENCE AS FOLLOWS:
                1.  APARTMENT
                2.  SINGLE FAMILY HOUSE
                3.  MULTI-FAMILY HOUSE
                4.  TRAILOR
4
ENTER THE LOCATION (MAX. 1 LINE).
3817 NORTH 16TH STREET
ENTER THE DAYS OF THE WEEK WHEN THE CRIME TOOK PLACE,
USING THE FOLLOWING CODE:

1.  SUNDAY     2.  MONDAY     3.  TUESDAY     4.  WEDNESDAY
5.  THURSDAY   6.  FRIDAY     7.  SATURDAY

ENTER A TWO DIGIT NUMBER WITH THE FIRST DIGIT BEING WHEN
THE CRIME MAY HAVE STARTED, AND THE SECOND WHEN IT IS
BELIEVED TO HAVE STOPPED.  FOR EXAMPLE,  IF THE CRIME MAY
HAVE OCCURED ANYTIME BETWEEN MONDAY AND FRIDAY, THEN THE
CODE WOULD BE AS FOLLOWS:      26
67
ENTER THE TIME WHEN THE CRIME MAY HAVE BEGUN AND THE TIME
WHEN IT STOPPED (MILITARY TIME). EX: 1700,1900
1000,2100
ENTER THE DATE WHEN THE CRIME BEGAN IN THE FOLLOWING FORM:
                EXAMPLE:  DD,MM,YYYY
                     14,9,1954 WOULD BE SEPT. 14, 1954.      4,4,1975
```

Figure 1

```
NOW INPUT THE METHOD OF ENTRY (MAX. 50 CHAR.)

KICKED IN THE BACK DOOR.
NOW INPUT COMMENTS (VEHICLE, SUSPECT). MAXIMUM 50
CHARACTERS PER LINE, 5 LINES.  IF YOU DO NOT NEDD ALL
5 THE TYPE A '-' ON EACH LINE.

VEG-HICLE:  WHITE MUSTANG
SUSPECT:  SUT--STUDENT OF SOUTHWEST TEXAS STATE.

TOTAL VALUE OF STOLEN ARTICLES = $200.

VERIFY YOUR DATA.

                                REPORT
-------------------------------------------------------------------
DISTRICT      RESIDENCE      DAYS            TIME            DATE
-------------------------------------------------------------------

 4            TRAILOR        FRI-            1000 AM.    4 4 1975
                             SAT             900 PM.

                  ----------------------------------------
        ADDRESS : 3817 NORTH 16TH STREET
          ENTRY : KICKED IN THE BACK DOOR.
        COMMENT : VEHICLE:  WHITE MUSTANG
                : SUSPECT:  SSTUDENT OF SOUTHWEST TEXAS STATE.
                :
                : TOTAL VALUE OF STOLEN ARTICLES = $200.
                :
                  ----------------------------------------


DO YOU WISH TO INSERT THE RECORD INTO THE FILE?  N
NOT INSERTING!
```

Figure 1 (Continued)

```
DO YOU WISH TO ADD A RECORD? N
DO YOU WISH TO WITHDRAW INFORMATION?    Y
WE ARE CURRENTLY ABLE TO SORT RECORDS ON 7 ITEMS.
YOU MAY SORT ON JUST 1 OR YOU MAY SORT ON ALL 7 OR
YOU MAY SORT ON ANY NUMBER IN BETWEEN.
WHEN I ASK IF YOU WISH TO SORT ON A CERTAIN ITEM PLEASE
RESPOND WITH YES OR NO.
DISTRICTS?N
RESIDENCE?N
DAYS OF THE WEEK?   Y
ENTER THE CODE AS FOLLOWS:
1. SUNDAY      2. MONDAY      3. TUESDAY      4. WEDNESDAY
5. THURSDAY    6. FRIDAY      7. SATURDAY
INPUT A TWO DIGIT NUMBER.  EX. 26 = MON-FRI        34
TIME?    N
DAY OF THE DATE?   N
MONTH OF THE DATE? N
YEAR OF THE DATE?  N
INPUT OF INFORMATION COMPLETE!

                                REPORT
-------------------------------------------------------------------
DISTRICT      RESIDENCE      DAYS              TIME              DATE
-------------------------------------------------------------------

 1            APART.         SUN-              1 AM.      1  1  1975
                             SAT               1200 PM.

                ----------------------------------------
        ADDRESS :516 BROADWAY, CORPUS CHRISTI TX. 78415
          ENTRY :BROKEN LOCK ON THE SIDE DOOR.
        COMMENT :VEHICLE:  1968 FORD CONVERTABLE
                :SUSPECT:  2 WHITE MALES.
                :THE PEOPLE WERE ON VACATION.  THEIR NEIGHBORS
                :SAW TWO MEN LOOKING AROUND THE YARD ABOUT
                :NOON THE DAY BEFORE.
                ----------------------------------------

 2            S HOUSE        MON-              1200 AM.   2  2  1975
                             FRI               1200 PM.

                ----------------------------------------
        ADDRESS :5209 LAMP POST LANE SAN MARCOS.
          ENTRY :BROKEN WINDOW
        COMMENT :VEHICLE-  UNKNOWN
                :SUSPECT-  UNKNOWN
                :
                :-
                :REFER TO REPORT 24464 FOR DETAIL INFORMATION.
                ----------------------------------------
THAT IS ALL THE RECORDS!
END -- POLICE RECORDS
DO YOU WISH TO ADD A RECORD? N
DO YOU WISH TO WITHDRAW INFORMATION?    N
READY
```

Figure 2

COMPUTER CRIMES*

Cropping up with disturbing frequency is a new brand of criminal specializing in theft by computer. The computer, in the hands of skilled operators bent on theft, fraud, or sabotage has become a major crime problem for business and government. In fact, experts believe that illegal use of computers is the fastest growing type of white-collar crime. Computer-related crime is difficult to detect. It is more profitable, less dangerous, and easier to commit than many other kinds of criminal activity.

The range of crimes made possible by computers runs from simple embezzlement to destruction of official information stored on data banks. Computer criminals have stolen trade secrets, valuable equipment and millions of dollars from banks, private companies and government agencies. Also, computers make excellent partners in crime because they do exactly what they are told and can be programmed to cover their tracks completely. (7)

Some of the cases recently uncovered are:

*A young graduate engineer in California used beep tones from his own touch telephone, to penetrate the computerized central-supply division at Pacific Telephone and Telegraph Company and steal over $1,000,000 worth of equipment. He spent the next three years selling the merchandise before an associate reported him because of a salary discrepancy.

---

*Report submitted by Mr. John Loyd to Dr. J. L. Poirot, SWTSU, Fall 1974.

*A chief teller at a branch of the Union Dime Savings Bank in New York was charged with embezzling 1.5 million dollars from the bank's deposits. He was caught when a bookie was raided and it was found that the teller had been gambling up to $30,000 a day. He was making $11,000 a year at the bank.

*An insurance company employee heard that he was going to be laid off, and programmed the computer to automatically erase the payroll tape when his employee identification number was dropped, resulting in a huge expense for the company. (7)

*In another case, a Salinas, California, accountant embezzled $1,000,880 from his company by recording higher payments for raw materials in the company computer than the company actually paid. He arranged for the computer to place the excess cash in his own dummy companies, and then programmed it to advise him how much money he could withdraw from those companies without raising suspicion. He was caught six years later when greed drove him to start making withdrawals of $250,000 a year. (6)

*A Washington, D.C., man takes the prize for elegant and successful simplicity. He pocketed all the deposit slips at the writing desks of the Riggs National Bank and replaced them with his own electronically coded forms. For three days, every customer who came in without a personal slip and used one of the "blank" forms was actually depositing money into the thief's

account. The thief reappeared, withdrew $100,000 and walked away. He has not been caught yet. (3)

*And then there was the Equity Funding case in which more than $60 million in counterfeit corporate bonds were allegedly counted among the assets of Equity Funding Corporation of America. (4) This is the biggest insurance swindle and one of the biggest swindles of any in history. In one of its subsidiaries, 58% of the 97,000 policies listed on the books were nonexistent. Also, on Wall Street, Equity Funding's more than 7,000 stockholders were in danger of losing at least $114 million; based on the deflated price of their stock. The greatest fact of this incident is that neither standard auditing practices nor Wall Street analysis was sophisticated enough to detect it. Equity Funding's fraud went to the extent of programming fake death certificates into the computer, to cover the fraud trail further. (2) Investigators found an office with 10 employees whose job was to simply forge documents. (4)

Now let's take a look at what sorts of people are involved in computer crimes. Donn B. Parker of Stanford Research Institute says that they are young and intelligent, usually between 18 and 30 years of age. They usually are not professional criminals. They are outwardly loyal and trustworthy and have never been in trouble with the law. They were in trusted positions before they committed their crime and are highly motivated and seem to be challenged by the prospect of beating a complex system

and overcoming protective devices, as much as by any monetary reward. Many computer criminals strongly believe that any information found unprotected in a computer is in the public domain and can be utilized by anyone who discovers it. Others rationalize that stealing from large corporations is not really a crime. Knowing what the criminals are like has not solved the problem. Mr. Parker says that spotting the crook before he commits a crime is next to impossible. (5)

For computer experts, this is the most disturbing aspect of the computer crime wave, that most of the culprits have been caught by accident. What makes these criminals so hard to catch is the extraordinary complexity of the computer programs themselves. The only sure way of detecting manipulations of such programs would be to devise another computer program capable of auditing the machines' internal operations. Unfortunately, no one in computer research today knows how to write such a program. Mr. Parker guesses that the ratio of undiscovered to discovered crimes may be on the order of a hundred to one.

For the time being, computer companies are restricted to improving the security systems inside their computers. Honeywell has devised a scheme called MULTICS, that restricts the total amount of information available to any individual user of a computer system. (6) In 1972, IBM began a $40 million, five-year program to improve its data-security systems. The National Security Agency and the Advanced Research Projects Agency of the Department of Defense are conducting independent research on protecting military and classified data stored on federal computers.

Moreover, the problem has given rise to a peripheral data-security industry made up of about 20 private companies. (7) Computer manufacturers are trying to develop systems that will be more resistant to manipulation. The consensus of the experts seems to be that it is possible to design penetration-proof operating systems, but that they are not likely to be commercially available in large systems in less than four years, at the earliest. Then they will have the problem of deciding what to do with the existing systems. Some advocate the use of separate minicomputers and software as gatekeepers, to handle the chores of user identification and access control. The main purpose is to remove these sensitive functions from the intricate maze of a main operating system. A number of companies are working on devices that will recognize personal insignia such as the shape of a hand or the unique motions an individual makes as he signs his name. While some companies are showing more and more interest in these new developments, other manufacturers contend that it's pointless to bring out systems capable of resisting sophisticated attack unless their customers adopt better physical security measures in their own installations, as well as better screening of computer employees. (1) Other computer crime preventing tips are to:

*Limit the number of employees who have access to the date stored in the computer.

*Switch computer users frequently to different machines and programs.

*Separate computerized check-writing operations from the departments that authorize checks.

*Use secret passwords to gain access to different computer programs and change the passwords often.

*Be sure the computer is programmed to sound an alert automatically when repeated attempts are made by computer users to enter incorrect passwords.

*Adopt procedures whereby those using the system have to enter their names or initials each time they have access to the system.

*Random monitoring of computer transactions.

*Provide detailed accounting of computer-usage time. If a job begins to take twice as long, analysis may indicate it is because the program has been modified to tamper with data files. (7)

A last approach for controlling computers crime is for companies to report the crimes and for the law to administer harsh punishment. Some banks and companies admit that when an incident is discovered, the corporate victims try to avoid the embarrassment and loss of confidence that publicity might bring.

About 85% of detected frauds are never brought to the attention of law-enforcement people. What often happens is that the offender, once detected, is required to make restitution and then leave - sometimes even getting severance pay and letters of reference to speed him away. (1)

Without adequate punishment the computer criminals will never be stopped. The electronics expert in Los Angeles, having served 40 days for his thefts from Pacific Telephone and Telegraph, is now back in business, advising clients on how to secure their computers against illegal entry.

BIBLIOGRAPHY

(1) Alexander, Tom, "Waiting for the Great Computer Ripoff," Fortune, July 1974, pp. 143-150.

(2) "Conning by Computer," Newsweek, April 23, 1973, pp. 90-91.

(3) "Key-Punch Crooks," Time, December 25, 1972, p. 98.

(4) "On the Coast-to-Coast Trail of Equity Funding," Business Week, April 21, 1973, pp. 68-72.

(5) "Spotting the Computer Crook," Science Digest, October 1973, p. 39.

(6) "The Computer Thieves," Newsweek, June 18, 1973, pp. 109-112.

(7) "Using Computers to Steal - Latest Twist in Crime," News and World Report, June 18, 1973, pp. 39-42.

THE NEED FOR COMPUTER SECURITY*

As the manipulation of data has been relegated to machine control more and more, there has been an increasing number of incidents involving the misuse of stored information. The most notorious of these incidents has chronically been that of Equity Funding, in which dummy records were created and stored on a computer system to pump up the "net" worth of the company.

This event, however, was but one of the occurrences. For the period between 1964 and 1972, the Stanford Research Institute has noted a total of 76 separate cases of sabotage, theft, copying data, tampering, masquerading, and fraudulent activities.[1] Of these, 61% were cases of theft and tampering with data alone.

As an indication of the already expanded use of data banks and other information storage and retrieval systems, one has only to look around him. Figure 1.1 gives an idea of the vastness of this use for only a few selected agencies.[2]

As files such as these are expanded and new ones created, the necessary considerations for keeping the data as well as the system that manages it secure must be incorporated in any EDP system.

*Report submitted by Mr. Fred Dickinson to Dr. J. L. Poirot, SWTSU, Spring 1974.

---

[1]Ruth M. Davis, "Privacy and Security in Data Systems," Computers and People, Vol. 23, No. 3 (March 1974), p. 25.

[2]Ibid., p. 24.

FILE MAINTENANCE AGENCY	NO. OF FILE SUBJECTS
Defense Department files	
Names of persons exposed to radiation	150,000
Family housing information system	465,000
Civilian personnel data bank	55,000
Defense industrial security programs	1,600,000
Navy manpower and personnel management information system	1,400,000
Justice Department files	
Civil disturbance file	13,000
Organized crime intelligence unit	200,000
FBI's National Crime Information Center	95,000
Other Government Agencies files	
National Driver Registration Service	2,600,000
Passport applicants of law enforcement interest	240,000
Banking Industry	
Bank of America individual accounts	14,000,000
Bank of America personnel files	41,000
Commercial Report Agencies	
TRW Credit Data	30,000,000
Insurance Companies	
Mutual of Omaha - applicant health records	8,500,000
Mutual of Omaha - benefit history files	5,000,000
Mailing List Companies	
R. L. Polk & Company names and addresses on file	200,000,000
College and Universities	
University of Maryland Personal & demographic records	158,000
Admission records	131,000
Accounts receivable from students	60,000

FIGURE 1.1

Provisions for Security

Basically, system security is the protection against the accidental or intentional destruction, disclosure or modification by a person who is unauthorized to do so.

Providing for this security can be thought of as a threefold project. First, proper management of the computer facilities is a must. A part of the reason the Equity Funding scandal succeeded is that there was no overseer of the company's programmers. Several programmers were given the initial assignment at Equity of generating model policies for the company. This included creating fictitious records as a part of the models. These modelled records were then sent to other programmers who were unaware that they were mere models, and the records were processed as though they were actual data. In a properly managed plant this could not have been possible.

In addition to the appropriate controls on the workers, care must be taken in deciding who is authorized to access a computer system, including its data storage. This encompasses the installation and maintenance of physical provisions for securing a computer system, which is the second of the three measures.

Some measures for material security include barriers preventing entrance to the actual computer area. Locks, gates, and alarms are already in use, particularly in applications where safety and security were a major concern even BEFORE the installation of EDP systems. Nowadays, restricting entry to a system involves not only such measures, but it incorporates the employment of guard personnel to check ID badges and oversee

the use of the system to prevent any misuse.

Devices that were originally designed to prevent accidental data destruction now play at least a minor role in security. Magnetic tape, for example, utilizes a write-lock ring to prevent writing when the ring is removed. Similarly, most Disk Operating Systems, as well as those using other system resident devices, have WRITE LOCK or WRITE ENABLE switches that control the function permitted on that peripheral device.

The final category of safeguarding an OS is through the application of software to monitor access to the system. Such software can, of course, be totally hardware independent, or it can function with peripherals designed expressly as protection devices.

Peripherals of this sort are primarily devoted to uniquely identifying a user in order to permit or deny access to the system. Systems already in use check punched or magnetic characters on a special card, such as those employed in the on-line operations just implemented for Master-Charge. In addition, there has been early research in detecting patterns in signatures, voiceprints and fingerprints. Measuring the length of a person's fingers, supposedly as identifiable as fingerprints, has drawn some interest.

Naturally, the control of similar devices could be granted to system software of the right variety. At present such programs already hold a protection function. In telecommunications environments, some Input/Output Control Systems are responsible for encrypting data prior to transmission. For the most part, this encoding is done by

adding/subtracting a random key number to the data at the transmission point. Upon reception, the same key number is subtracted/added to yield the original data. While such a key number algorithm can theoretically be broken, it provides a degree of protection in that only sender and receiver really know the key. To prevent accidental disclosure, the machine itself can be programmed to perform the encryption. To aid in the spread of this coding practice, the National Bureau of Standards plans to make encoding algorithms available by fiscal year 1975.[3]

Monitors in timesharing systems further serve in identifying users and in recording the essentials of a users account (time used, cost and the like). When a user attempts to log onto a system, the supervisor usually calls a routine that checks a master file for the identifier, or user number. If it is a valid number, the user's account is checked to see if his password is valid and his account is not overdrawn. If these checks are alright, the user is permitted to continue. Where certain devices require serial processing and are protected by the use of passwords, a similar search routine is called so the monitor can deny or permit access.

A splendid example of such file protection exists by considering the use of protect (or access) codes. The PDP 11/20, manufactured by Digital Equipment Corporation, utilizes the protect codes as outlined in Figure 2.2 and demonstrated in 2.1.[4] The directory shown in 2.1. shows

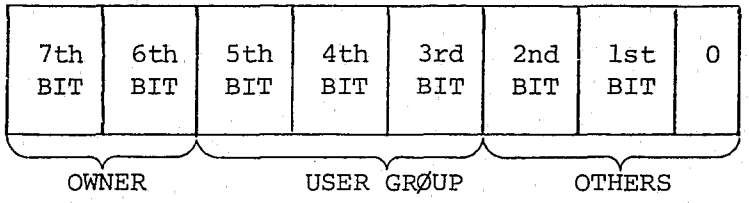
---

[3] Ibid., page. 27

[4] File Utility Package Programmers Handbook, DEC, August 1973, p. 3-12.

```
DISK  [20,20]

DIRECTORY DKØ:  [2Ø,2Ø]

Ø1-Apr-74                                          CREATION DATE

RRFLIB.OBJ     26    16-JAN-7Ø <233>
MEBLIB.OBJ     24    17-JAN-7Ø <233>
BAJØ7 .OBJ     33    16-JAN-7Ø <233>
GLORIA.OBJ      8    17-JAN-7Ø <233>
KSR   .OBJ      1    17-JAN-7Ø <233>
GLORII.OBJ      8    19-JAN-7Ø <233>

TOTL BLKS:    1ØØ
TOTL FILES:     6

                                                   PRØTECT CØDE
FILE NAME
```

FIGURE 2.1.



OCTAL NUMBER	FUNCTIØNS PERMITTED USER			
	DELETE	WRITE	READ	RUN
0	YES	YES	YES	YES
1	NO	YES	YES	YES
2/3	NO	NO	YES	YES
4/5	NO	NO	NO	YES
6/7	NO	NO	NO	NO

FIGURE 2.2

the files, their lengths, creation dates (in this case, the dates are default dates for the system), and the access codes for the disk area with a user identification code or [20,20]. The protect code for the PDP is a three digit octal number in which the 6th and 7th bits indicate functions permitted the owner, and the bits 0-5 denote functions allowed other users using [20,20]. The chart in Figure 2.2. explains the details of choosing a code to be assigned a file.

Data Securing Engineering

As the utilization of automated data systems increases, there will be an increasing concern for "intruder interactions" and the engineering and programming capacity to deal with it.[5] To stave future episodes of Equity Funding, auditing and control programs are being developed. Cullinane Corporation has already marketed an EDP Auditor and a Culprit package that uses a series of monitor programs to control access to their systems.[6]

To prevent physical tampering, basic designs have been altered in a few cases. The Basic Computing Arts, Inc. of Palo Alto, California, markets a system comprised of a minicomputer and a larger host computer (an IBM 360 or 370).[7] This Data Sentinel has the minicomputer sealed in a "tamper-proof" case and tapped with alarms and a single relay to the host. In this case, the mini performs the guardian functions of user identification and checking the legitimacy of all software. One of the singular applications of this system, installed at the Crocker National Bank in San Francisco, authenticates software by a check sum algorithm and comparing this sum to a stored total input when the software is first implemented. If the two sums check, the program is permitted to be executed by the host computer.

One of the systems now lauded as extremely secure did not even begin as a security concern. Honeywell's MULTICS system, developed in conjunction with MIT and the Bell Labs and now available on the Honeywell

---

[5] Computer Abstracts, Vol. 17, No. 10 (October 10, 1973, number 2521.

[6] "Outwitting the Computer Swindler," Computer Decisions, Vol. 5, No. 9 (September 1973), p. 15.

[7] Ibid., p. 16.

6184, has a file structure that provides the added security now hailed. In the system files are divided into segments and arranged hierarchically in concentric circles. The innermost rings, containing the monitor and vital system software, is accessible only by the MULTICS system itself. Outer rings are available for users. By selecting the appropriate access code (and thereby the segment) a user determines the degree of file protection desired.[8]

Advancements such as these will no doubt continue; however, careful analysis of a systems needs is necessary since costs increase as security measures are implemented. For example, the MULTICS system, including CPU and a number of peripherals, can cost upwards of $1.5 million. Furthermore, as checks of users to determine accessibility increase, the efficiency of a system is decreased due to the time necessary for table and file searches. In addition, with the implementation of federal laws governing data protection, file sizes will no doubt increase, thus requiring more storage devices. Soon, files on persons (data banks, credit bureaus, etc.) will be forced to contain source listings, creation dates, list of those eligible to access that file, and other related information. It has been estimated that, considering such required information and a probable growth in numbers of files of 10%, the files on people in existence would double in size in only seven years.

Considering the present clamor over protecting data systems,[9] it is hardly necessary to expound on its importance. Effective data security engineering is and will be of great concern to all who use EDP systems.

---

[8]Ibid., page 16.

[9]Davis, Computers and People, page 25.

BIBLIOGRAPHY

1. Computer Abstracts, London, Technical Information Company, 1973, Volume 17, No. 10.

2. Davis, Ruth M., "Privacy and Security in Data Systems," Computers and People, Volume 23,3, March 1974, pp. 25-27.

3. Digital Equipment Corporation, DOS/BATCH File Utility Package (PIP) Programmers Handbook, Monitors Version V09, August 1973, pp. 3-12.

4. Feistel, H., "Cryptography and Computer Privacy: protecting personal data banks," Scientific American, 228, May 23, 1973, pp. 15-23.

5. "Outwitting the Computer Swindler," Computer Decisions, Volume 5, No. 9, September 1973, pp. 12-16.

END