1-1-1975

Defining computer security needs in a university data base environment.

Leslie D. Ball
University of Massachusetts Amherst

DEFINING COMPUTER SECURITY NEEDS IN A UNIVERSITY DATA BASE ENVIRONMENT

A Dissertation Presented

By

LESLIE DAVID BALL

Submitted to the Graduate School of the
University of Massachusetts in partial
fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

JUNE 1975

Major Subject: Business Administration

DEFINING COMPUTER SECURITY NEEDS IN A UNIVERSITY DATA BASE ENVIRONMENT

A Dissertation

by

LESLIE DAVID BALL

Approved as to style and content by:

Van Court Hare Jr.

Van Court Hare, Jr., Professor, Department of Management, SBA Chairman

John G. Burch Jr.

John G. Burch, Jr., Associate Professor, Department of Accounting, SBA, Member

Hugh J. Miser

Hugh J. Miser, Professor, Department of Industrial Engineering & Operations Research, Outside Member

George S Odiorne

George S. Odiorne
Dean
School of Business Asministration

June 1975

DEFINING COMPUTER SECURITY NEEDS IN A UNIVERSITY DATA BASE ENVIRONMENT

Leslie David Ball
B.S., Northeastern University
M.B.A., Boston College
Ph.D., University of Massachusetts

Directed by: Dr. Van Court Hare, Jr.

Abstract

Despite significant advancements in the solving of computer security problems, it has been reported that over 90% of all computer installations have inadequate security. A contributing factor to this phenomenon has been the user's inability to adequately determine his security needs. To remedy this situation, it is essential to develop analytical tools to define security needs in differing user environments.

The purpose of this dissertation was to investigate four methods for defining computer security needs in a university data base environment. The methodology employed was that of an exploratory field study.

In Chapter II, the literature was reviewed. The interrelation of privacy issues and computer security problems was developed and security problems were classified. James Martin's Security Exposure Rating and Rein Turn's Value of Information Measure were presented as possible alternatives for defining computer security needs.

A contemporary view of data base design and the factors to be considered in developing a data base security model were presented in Chapter III. Data organization in a data base, key characteristics of data base design, and problems unique to data base design were presented as background to the problem. It was pointed out that the relationships of Turn's four design criteria (effectiveness, economy, simplicity, and reliability) for an effective security plan are not clearly understood. Further, an objective function must be decided upon before such a plan can be developed. Constraints suggested are the value of the information stored in the data base and the cost of the protection plan.

Presented and analyzed in Chapter IV were the four methods for defining computer security needs as well as a major control problem uncovered in the course of the study. The student data base at the University of Massachusetts served as the test facility.

First, major users of the new data base were interviewed. They were asked to determine the effect of accidental or intentional destruction, modification, or disclosure of data elements on the operation of their departments. In general, it was found that this was an inadequate method for defining security needs as few users were able, or even willing, to consider the consequences of various events occurring.

Second, the actual structure of the data base was de-

fined. It was suggested that by determining which users have authority to create, to access, or to update data elements that basic security needs would be uncovered. The information developed from this method is necessary for the creation of authorization matrices but not sufficient for the development of a complete security plan.

Third, the actual usage of data elements in the data base was determined. It was suggested that valuable information about the usage of the data base would be determined. This information could be used for defining backup procedures and access monitoring but, again, failed to provide sufficient information to develop a complete security plan.

Finally, the actual usage of the computer system was investigated. It was found that user departments vary in the manner in which they use the system and the time periods in which their heaviest usage occurs. This provided information about peak usage periods which is necessary for the development of an adequate security plan.

While none of the four methods clearly defined security needs in a university data base environment, each one provided information necessary in the creation of an adequate security plan. It was concluded that needed is a procedure for the logging of security breaches which would eventually be employed to develop occurrence probabilities.

In Chapter V the limitations of the study were presented. Recommendations for further research were also suggested.

ACKNOWLEDGEMENTS

I would like to thank a number of people for their encouragement and support during the preparation of this dissertation. Professor Van Court Hare, Jr. has served as both my doctoral program advisor and as chairman of my dissertation committee. He has always been most generous with his time and with his guidance.

Professors John G. Burch, Jr. and Hugh J. Miser also generously contributed their comments and assistance in completing this dissertation. Their help was also significant.

To the people in Management Systems and the other people in various departments whom I interviewed I thank them for their assistance. Special thanks goes to Bard White, Robert Baron, and Martha Little for without the large blocks of time that they gave me this dissertation would have been impossible.

To Mrs. Vesta Powers I would like to extend my thanks. Her cheerfulness and competence in typing the final copy greatly helped me to complete the dissertation.

Lastly, but not least, to my wife, Martha, I owe a great deal of thanks for typing, proofreading, and loving support during this difficult project. Because of her dedication to me, this dissertation is dedicated to Martha and a future "computer jock," Jennifer.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

C H A P T E R I

INTRODUCTION

The Problem In Perspective

Since the early 1960's the concern about computer security has grown rapidly. During this period of growth the computer's use has grown to a point where many organizations are now dependent upon the computer's functions to carry on their work. To insure that the computer remains in operation it is important that security be given appropriate consideration in the development of any information system.

Security can be defined to apply to data security or computer security or some combination of both. Data security is defined by Turn and Shapiro as the protection provided for the databank system against deliberate or accidental destruction, and unauthorized access or modification, of the data.[1] Computer security may be defined as the protection of the hardware from loss due to fire or some other unfortunate event, but information systems require that the computer system and the data that it stores be protected against threats from the environment.

Over the course of the last decade a great amount of effort on the part of computer manufacturers, computer users, and independent researchers has been directed to developing secure computer systems. Early efforts were directed at

identifying potential threats to computer systems and an enumeration of possible countermeasures to prevent these threats from occurring.[2] From that base, a number of operating systems were written which contain data security features.[3] Physical security considerations have become well defined[4] and checklists have been developed[5] which aid the user in implementing various security measures.

The design and implementation of a security plan will remain more of an art than a science until adequate theoretical foundations are laid and analytical tools developed for a "data security engineering" discipline.[6] Needed in particular are measures for evaluating the effectiveness of data security techniques in various threat situations, methods for estimation of the costs of implementing the safeguards in various classes of information, and exploration of tradeoff relationships between these and other relevant variables. Equally important is the ability to estimate potential losses.[7]

The security needs of each computer system and computer user vary based on the complexity of the computer system, the types of applications, and the value of the data stored and processed by the computer system. Therefore, a security plan must be individually tailored for the particular needs of the computer user.

Recently, data bases have become more popular. Security needs for a data base differ from traditional data pro-

cessing techniques because of the availability of the on-line accessing capability, the storage structure of data, the dependence of one user's actions on another, and a host of other capabilities unique to data base design. Computer users, beginning to use data bases, may find that the security plan that was previously adequate will not be sufficient. Additional research is required to develop analytical tools for determining these additional security needs.

Purpose of The Study

The purpose of this study is to investigate four possible alternatives for determining security needs in a data base environment. In particular, a university computer system will be employed for this field study.

Significance of The Study

Little is currently known about the effectiveness of various security plans. The reason for this is that security plans have not been developed to meet a defined set of needs, and no one has been able to establish procedures for determining these needs.

As the determination of security needs should be the first step in the design and implementation of any security plan, this study should aid in eliminating the "seat of the pants" approach currently in use by many data base users.

By so doing, it will also help the creation of a more cost-effective security plan.

Structure of The Report

In addition to this chapter, the report contains four other chapters. Chapter II will present a discussion of the most relevant literature relating to security issues. Many of the important factors in all security plans will be presented in this chapter.

Chapter III will present a discussion of the theoretical considerations of defining a complete security plan. In Chapter IV the four suggested alternatives for defining security needs in the student data base at the University of Massachusetts will be presented.

Finally, Chapter V will summarize the significance of this work and its basic limitations. Along with this material will be a general discussion of areas for further study.

Footnotes

[1]Rein Turn and Norman Z. Shapiro, "Privacy and Security in Databank Systems: Measures of Effectiveness, Costs, and Protector-Intruder Interactions," Fall Joint Computer Conference, Vol. 41, Part I (Fall, 1972), 436.

[2]H.E. Petersen and Rein Turn, "Systems Implication of Information Privacy," Spring Joint Computer Conference, Vol. 30 (Spring, 1967), 291-300.

[3]For example, see: Edward L. Glaser, "A Brief Description of Privacy Measures in the Multics Operating System," Spring Joint Computer Conference, Vol. 30 (Spring, 1967), 303-304.

[4]Dennis Van Tassel, Computer Security Management, (Englewood Cliffs, N.J.: Prentice-Hall, Inc., 1972).

[5]Leonard I. Krauss, SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems, (East Brunswick, N.J.: Firebrand, Krauss and Company, Inc., 1972).

[6]Turn and Shapiro, Ibid., 435.

[7]Ibid.

C H A P T E R II

COMPUTER SECURITY IN REVIEW

Introduction

Definition of privacy. The term privacy is often incorrectly used as a synonym for computer security. Much of the confusion stems from the 1967 Spring Joint Computer Conference when Willis Ware introduced a session on security and privacy by defining the terms security and classified to refer to defense or military information or situations while private and privacy were used in reference to corresponding industrial or non-military governmental situations.[1] Ware's original framework is not now the currently accepted definition of either privacy or security.

Early references to privacy in U.S. law appear in a decision by Justice Louis Brandeis. He defines privacy as the "right to be left alone."[2] Further, Brandeis indicates that this right is "the right most valued by civilized men."[3] Most legal references to privacy since the early 1900's have been based on the Brandeis decision. At about the same time that Ware was defining privacy, Alan Westin defined it as:

> "...the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[4]

However, Peter Browne defines privacy as the guarantee to

the proprietor of a file that information contained therein is not made available to unauthorized users.[5] Perhaps, Rein Turn's definition of an individual's right to privacy--his right to determine for himself what personal information to share with others[6]--is a good blending of Westin's and Browne's definitions. This is particularly true if we define "share" as providing the information originally and then allowing dissemination of it.

It is clear, then, that computer privacy relates to the sharing of information about oneself with others. It is not clear, however, how one determines when an invasion of privacy by computer has occurred. This determination must be made in the courts or by legislative actions.

Definition of security. The enforcement of laws, rules and procedures to maintain a secure data base[7] is the definition of security used by Stewart Madnick at MIT. A monograph published in 1968 by IBM Corporation defines security as the "protection of data from accidental or intentional disclosure to unauthorized persons and from unauthorized modification."[8] Richard A. Hirschfield views security as a problem of comprehensive computer control and, further, makes the assertion that most companies do not have it.[9]

R.W. Conway, W.L. Maxwell, and H.L. Morgan show that information security involves the question of procedures to insure that privacy decisions are, in fact, enforceable and enforced. They warn that computer professionals must insist

that a security system be an integral part of any information system containing potentially sensitive data or the computer profession will soon find itself with the same problems of conscience that nuclear physicists suffered in the late forties.[10]

The term "data security" has recently been coined. Robert Courtney says that data security refers to the safety of data from all of the unfortuante things which can happen to it, like accidental or intentional, but unauthorized, modification, destruction or disclosure.[11] Turn's definition is a bit more encompassing. He says that data security is the protection of the computer system resources against unauthorized access, use, modification, or destruction, as well as against attempts to prevent authorized use of the system.[12]

The definitions of security and data security, are more concrete than the definition of privacy. Although analysts developing a security plan must be concerned with preventing the modification or destruction of data, they cannot forget that information will be shared, which requires that the relationships between privacy issues and security issues be clearly understood before comprehensive security systems can be developed.

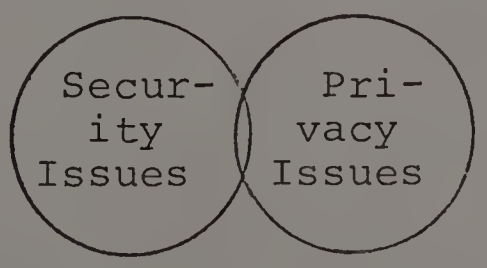
Privacy and security relationship. The relationship between privacy and security is not well defined. Security is a systems problem and privacy is a legalistic and/or

moral issue. Security is concerned with unauthorized access to data, but so is privacy. Preventing the unintentional alteration of data is a security concern, but when data is altered it could be a privacy issue.

For example, consider the case of a disgruntled programmer employed by a credit reporting agency. Before leaving the firm's employment, assume that he modifies a computer program to systematically alter credit files. In addition, assume that this is not uncovered until a large number of people have been denied credit based on these modified ratings.

An invasion of privacy has occurred as well as a security breach. The privacy invasion resulted from incorrect information being supplied about individuals and the security breach occurred when the programmer modified the program. Adequate controls could have prevented this situation which clearly involves both privacy and security.

If we could enumerate the entire set of issues under the headings security and privacy we would find some overlap. The extent of that overlap and the size of each set is open to discussion and further research. However, the two problems in abstract form appear quite like Figure 2-1



Security and Privacy Relationships

Figure 2-1

Martin has suggested that privacy cannot be insured without security, and most of the technical methods of achieving privacy are also essential for security.[13] This supports the relationship stated above. But can a secure system insure privacy? The answer could be no if a totally secure system is used to store personal information on individuals and that information is used improperly. An example of such a system might be a credit reporting agency that fails to allow the consumer to correct his records. In systems development, analysts must be concerned with two questions: 1) will this system insure the individual's privacy? and 2) does use of this system constitute an invasion of the individual's privacy? All systems must be developed with heavy emphasis on security but still maintain a proper balance between the two issues.

Interest in computer privacy issues has intensified to the point that President Gerald Ford signed a bill into law on December 27, 1974, which regulates federal databanks.[14] Although security is the main issue of this study, its relationship to privacy and the increased government concern requires that an underlying consideration be given to privacy in developing solutions to all security problems. While in the remainder of this chapter the most important security problems will be examined, privacy will only be discussed when it directly applies to the particular security problem being presented.

The organization found in the remainder of this chapter is not historical. Research on security and privacy issues has been occurring along many fronts during the past decade which makes it difficult and confusing to attempt to present this research in chronological order.

Instead, the next section will present a discussion of threats which are defined as any event that can cause harm to the computer or data stored in the computer. Then a presentation of the most important classes of countermeasures, which can be defined as any device or procedure that can prevent a threat from occurring or minimize its effect should it occur, will be given. While logic might suggest that threats and countermeasures be paired up they cannot always be matched so the subjects will be discussed individually.

Following the discussion of threats and countermeasures, some miscellaneous topics will be presented. Finally, a summary of the security problem will be presented.

Threats

Much of the early work in computer security was in the development of possible threats to the computer system and the data that the system stores. At the Spring Joint Computer Conference in 1967, Ware introduced the first session to have ever been presented on computer security to the computer conference. He presented a figure of a typical

resource-sharing computer system (Figure 2-2) and explained where threats originated.[15]

Ware enumerated a number of threat sources: 1) failures in hardware and software, 2) intruders attempting to tap communication lines and pick up system radiation, or 3) illegally accessing, copying, or stealing files. Of prime importance, Ware emphasized, are threats originating from personnel within the computer center. Operators, programmers, and maintenance engineers have freer access to the system than other groups of individuals which gives them more opportunity to breach the computer system.[16]

Threat seriousness, Ware continued, depends on the sensitivity of information being handled, class of users, operating environment, and design skill of the systems developers. Systems developers must protect against all types of invasions suggested plus those not yet conceived.

H.E. Petersen and Turn classify threats as accidental or deliberate. Examples of accidental threats include operation errors and "Acts of God." Further, they classify deliberate disclosures as either passive or active.[17] For example, wiretapping or electromagnetic pickup is passive. Theft is active. According to Petersen and Turn, communication lines are the most vulnerable system part for both active and passive threats.[18]

Risk measurement. Risk measurement is not easy. Each computer installation presents several possible risks or

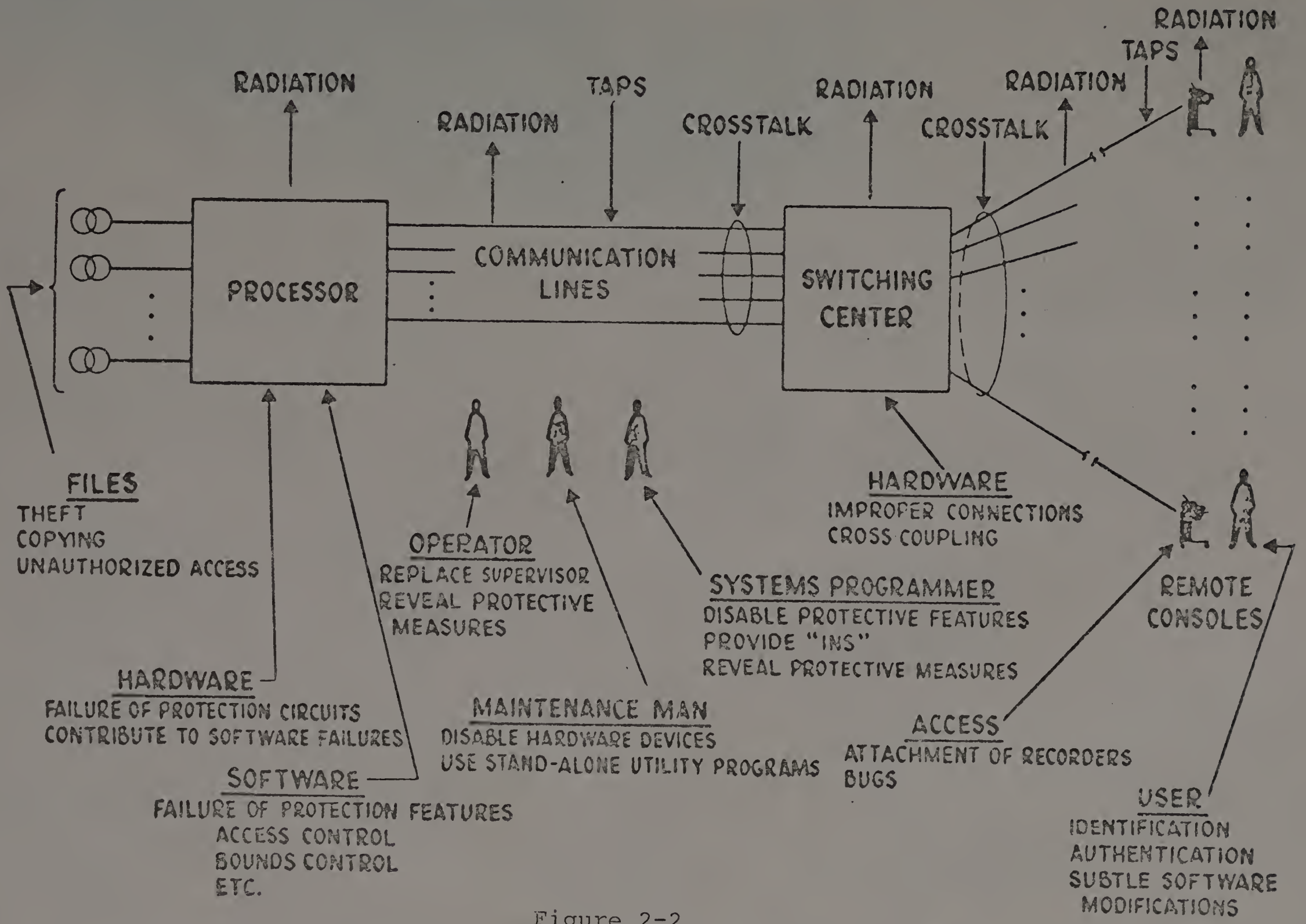


Figure 2-2

Computer Network Vulnerabilities

threats. Associated with each risk is a difficult-to-measure occurrence probability. Yet, we must measure potential risk to insure adequate security.

Richard B. Canning and Robert Courtney suggest that rough estimates and guesses make more sense than no estimate at all.[19] Courtney shows that the economic value of any protective device often exceeds its cost--even if we overestimate the threat probability.[20]

James Martin suggests a relatively simple procedure for determining a "security exposure rating."[21] (See Table 2-1) First, the user should establish a matrix to list possible threats down the side and results, such as "inability to process" and "loss of single records," across the top. Next, the matrix would be filled in for each application with a rating for the approximate probability of an event occurring, P, as defined in Table 2-1.

Table 2-1

Probability Ratings

P: Rating for the probability of an event occurring:

0: Virtually impossible

1: Might happen once in 400 years

2: Might happen once in 40 years

3: Might happen once in 4 years (1000 working days)

4: Might happen once in 100 days

5: Might happen once in 10 days

6: Might happen once a day

7: Might happen 10 times a day

A duplicate matrix will be filled in with a rating, D, for the amount of damage the event causes in lost business, cost of correcting the data, and other costs as approximated in Table 2-2.

Table 2-2

Damage Ratings

D: Rating for the amount of damage the event causes in lost business, cost of correcting the data, and other costs:

0: Negligible (about $1)

1: On the order of $10

2: On the order of $100

3: On the order of $1,000

4: On the order of $10,000

5: On the order of $100,000

6: On the order of $1,000,000

7: On the order of $10,000,000

Finally, the exposure rating, E, is obtained for each event from:

$$E = \frac{10^{(P+D-3)}}{4} \quad \text{dollars per year when P and } D \neq 0.$$

E provides a measure for determining which problems should have the greatest attention paid to them.

A different approach is suggested by Javier Kuong.[22] His "risk analysis and evaluation of protection programs"

is presented in Figure 2-3.

To employ Kuong's procedure, the user must first prepare a list of all possible threats that might occur. For each threat an estimate of the cost of impact of the threat must be made and an estimate of the frequency, or the probability of occurrence, made as well. When three estimates of each are used, the expected cost of the event, C_1, and the expected risk, R_e, are calculated as:

$$C_1 = \frac{a+4m+c}{6} \quad , \quad \text{and}$$

$$R_e = \frac{a+4m+c}{6}$$

where a is the minimum estimate, c is the maximum estimate, and m is the middle estimate. Otherwise, C_1 and R_e are the original estimate.

The expected loss, C_E, for that threat is found from:

$$C_E = C_1 \times R_e$$

The user should determine all alternative protection methods and select the one that he believes to be most effective in fighting off this threat. Its cost estimate will be C_p. Any intangible factors in favor of protection will be quantified as C_{IN}. Finally, the incentive for adopting the protective measure, I, is obtained from:

$$I = C_E - C_P \ (+C_{IN})$$

As stated before, this procedure is done for all threats. The user should then adopt all protective measures

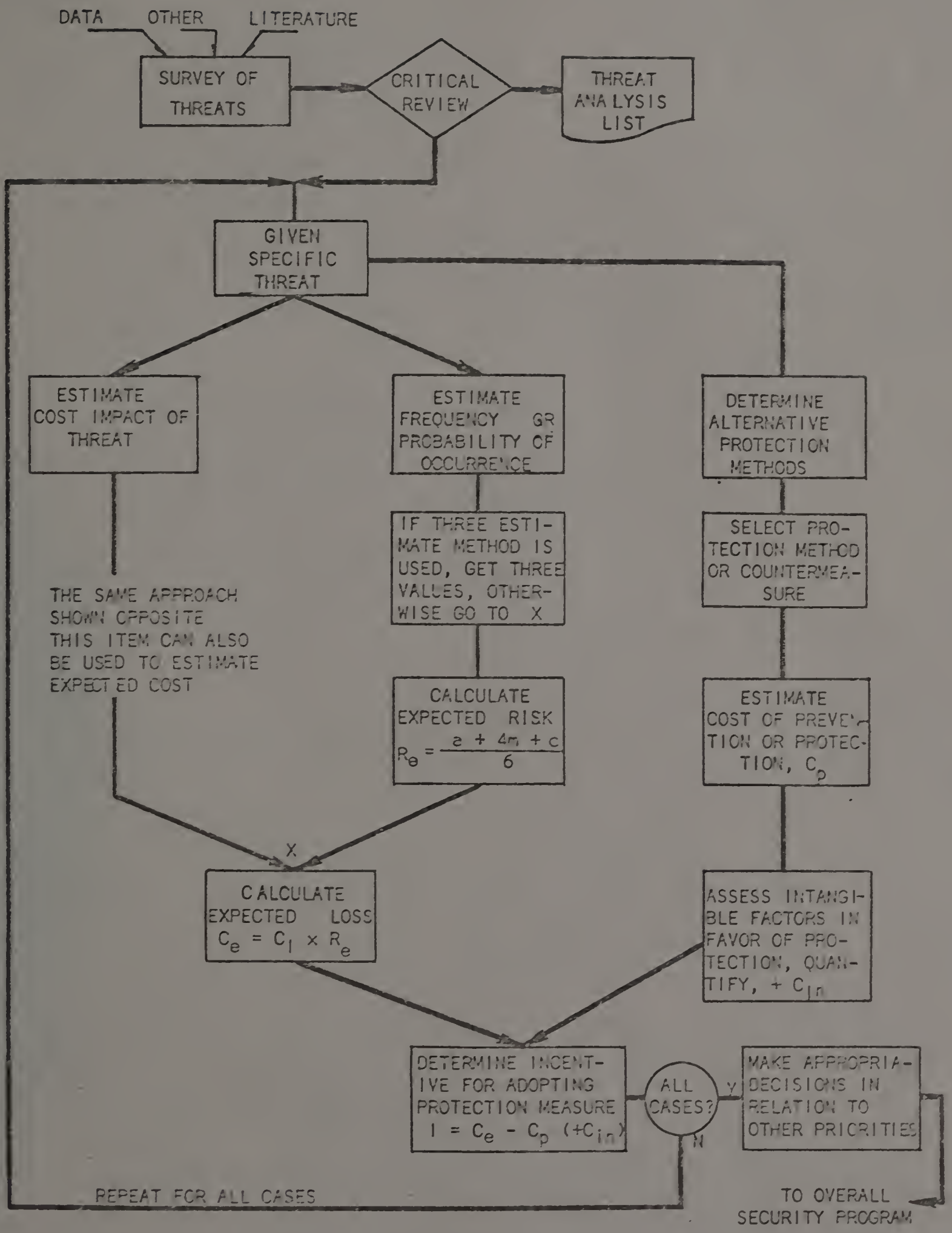


Figure 2-3

Risk Analysis And Evaluation of Protection Programs

for which I > 0 unless, of course, other priorities must be considered.

A Mathematical model of protector-intruder strategies is suggested by Rein Turn and Norman Z. Shapiro which requires that the value of information stored in the data base to the protector and to the intruder be estimated.[23] As an example, they select a "mailing list," L, of N information items, each of which has the market value k. The total market value of L is:

$$V = kN$$

If the intruder must make an investment, X, to penetrate the data base and requires a minimum profit, rX, where r > 0, then his maximum investment to obtain L is:

$$X = kN/(1+r)$$

To counter this threat, the protector spends Y resources on data security measures, so the problem becomes one of determining Y.

Let I(X,Y) be the expected amount of information obtained by the intruder when he expends X amount of resources to overcome Y amount invested by the protector. Some of the elementary properties of I(X,Y) are:

$$I(O,Y) = I(X,\infty) = 0 \text{ , for } X,Y > 0$$

I(X,Y) is monotone non-decreasing in X and monotone non-increasing in Y.

Letting f(N) be the value to the intruder of N units of in-

formation and g(N) be the cost to the protector and subjects of the same N units of information, the expected net profit of the intruder, v(X,Y) is:

$$v(X,Y) = f(I(X,Y))-X$$

while the net loss to the protector and subjects, u(X,Y), is:

$$u(X,Y) = g(I(X,Y))+Y$$

Given that the intruder would want to maximize his profit, he would vary X until v(X,Y) is at a maximum. Conversly, the protector would want to minimize u(X,Y) by varying Y. The selected values of X and Y will satisfy:

$$f'(I(X,Y))\partial I(X,Y)/\partial X=1, \text{ and}$$

$$g'(I(X,Y))\partial I(X,Y)/\partial Y = -1$$

Of course, the Turn and Shapiro approach requires that many analytical or empirical expressions be developed to express these relationships, many of which might be difficult to construct. Although their model is built on the value of data to a possible intruder, it might be possible to modify the model slightly to substitute the cost of reconstructing in the event of a fire or some other threat for the intruder's investment, X.

It is apparent from the above discussion that the measurement of risk is much more of an art than a science. The great number of possible threats that must be enumerated in the Martin and Kuong approaches comprise an infinite list. Even selecting the ones most applicable to a particular in-

stallation is extremely difficult.

While Turn and Shapiro offer a different approach, the measurement of the market value of data is often difficult. All three approaches offer interesting starting points to additional work that must be done to refine the processes.

Research and statistical databanks. With the great amount of data collected for research or statistical purposes increasing rapidly, the concern over what that information will be used for is also increasing. People are beginning to believe that by answering questionnaires they are creating a threat to their own privacy. Social researchers are aware of this problem and believe that unless they are able to keep identifiable data confidential that their ability to collect data will suffer.[24]

This problem has long been a concern of the United States Bureau of the Census. In fact, the census law (Title 13, U.S.C., Sec. 9-a-2) provides that there shall not be any publication (or other revealing of information) whereby the data furnished by any particular establishment or undividual under this title can be identified.[25] Although the census bureau has an unblemished record, a number of suggestions for concealing research data have appeared. One suggestion is to randomly modify data that is distributed for statistical purposes.[26] This would not affect the research outcome but would mask the raw data.

1. dossier information

A procedure employing statistical data to ascertain dossier information was described in an article by Lance Hoffman and W.F. Miller.[27] They contend that if we know a number of properties about an individual we can use the databank to find out additional information. Say, for example, we want to know if John Doe earns over $50,000 per year. We know that he is a 39-year-old lawyer living in New York City with his second wife and their four children. We can ask the data bank, "how many people are there in the data bank with the following properties:

Age 39
Education level LLB
Male
Has four children
Lives in New York City
Profession is Lawyer
Has been married twice?"

Assume it responds with the answer "57 people." Then we ask the same question but add the property "salary exceeds $50,000 per year." If the response is "57" we then know that he earns greater than $50,000 per year.[28]

Similar questioning can create an entire dossier on the individual in question. In fact, if the properties selected yield a cell size of one, then those inquiries with one additional property will return a "1" if the property is true and a "0" if the property is false.[29] To protect against this type of disclosure is nearly impossi-

ble and many would say that it is impossible.[30] Hoffman and Miller suggest that threat monitoring might be the only way to protect against this type of attack.

2. Private information

As the researcher creates his data base he must not attempt to collect data in a way that might be thought of as privacy invasion. Although no definitive statement exists which provides a clear statement of what is "private information," or what constitutes an "unwarranted invasion of privacy," Edward V. Comber[31] has suggested that researchers must take into account whether or not disclosure of the specific data: 1) would relate to an individual, a family or other small group in such a manner as to increase the probability of the unwarranted identification of the individuals, or 2) the data is not considered public information by provision of legal statute, or 3) would cause or be the basis for unjust economic loss or social stigma or harrassment to the individual, or 4) result in the unnecessary loss of a property right.

Threats, as has been shown, include threats to the computer system as well as threats to an individual's privacy. Many of them are caused by the computer environment but a great number result from humans attempting to use the computer system improperly or to access data which they are not authorized to see.

It is impossible to enumerate all threats. It is, however, possible to classify threats and suggest countermeasures for various classes of threats from the environment or from humans.

Countermeasures

To thwart a threat to the system, Petersen and Turn offer five classes of countermeasures: 1) access management, 2) processing restriction, 3) threat monitoring, 4) privacy transformations, and 5) integrity management.[32] Access management is defined as preventing unauthorized users from obtaining services from the system or gaining access to its files. Included in this class are such things as the use of passwords and various other authorization techniques.

Processing restrictions, imposed on files containing sensitive information, are used to protect files from access or illegal alteration. They can also be used to prevent users from accessing various sections of storage in which sensitive information or the operating system might reside.

Threat monitoring is the detection of attempted or actual penetrations of the system or files either to provide a real-time response or to permit ex post facto analysis. Included in this class of countermeasures are audits and logs which can provide "alarms" to an attempted penetration or an ongoing attack.

The fourth countermeasure, privacy transformations, in-

cludes techniques for coding the data communications between the user and the processor or concealing the actual information held in certain files. Petersen and Turn point out that this countermeasure offers substantial protection against certain threats but also note the increase in processing required of the system.

The final class, integrity management, refers to the verification that the system software and hardware perform as specified and includes the verification of the performance of personnel and the communication channels. This is the most difficult class of countermeasures to develop.

Physical security measures. Physical security measures have been discussed extensively in the computer trade journals, but little mention is made of them in academic journals. This can be explained by noting the mundane usage of physical security measures. Research cannot be done by computer scientists to determine the best lock to be put on a computer room door or the most effective vault type for the storage of backup files.

Perhaps another reason that academicians do not study physical security measures is that there isn't much more that needs to be known about them. Their costs are easily estimated and the effectiveness of the devices has been determined to meet defined specifications leaving little mystery about them.

However, physical security measures are important, even

if they are mundane. They must be considered as part of any security plan. Without some basic physical security measures, large funds put into securing the operation system or enciphering data files are worthless.

James Martin breaks physical security problems down into six distinct areas and devotes a chapter to each. These chapters are: 1) Locks, Vaults, and Protected Areas, 2) Electronic Security Devices and Systems, 3) Fire and Acts of God, 4) Sabotage, 5) Communication-line Wiretapping, and 6) Electromagnetic Radiation and System Eavesdropping.[33]

In the first chapter, Martin discusses what types of things should be in a protected area and how it should be protected. He includes the National Fire Protection Association recommendations for vaults[34] and considerations about locks and fire alarms.[35] All of these items are described in numerous other sources[36] and several "horror stories" have demonstrated the value of the devices.[37]

A number of electronic security devices and systems are marketed to prevent a variety of threats to the computer center. Those devices include burglar alarms, fire detectors, water-flow detectors, and remote controlled television cameras. Martin discusses each of these and their applicability.[38]

Threats from fire and Acts of God, most feared by data processing managers, can be minimized by employing effective physical security measures and locating the computer in-

stallation in a less vulnerable location. Publications about these disasters have been directed at preventing them from happening and, if they should occur, minimizing the potential loss.

Few computer installations protect against sabotage, yet virtually every installation is threatened by possible sabotage. In one manufacturing firm, power to the computer center was cut by a man whose sister was killed in an automobile accident on the way to work.[39] This act resulted from the confused belief of the saboteur that because the woman worked for the company that a destructive action would vindicate her death. This example, and many similar instances, demonstrate the difficulty of protecting against sabotage.

Communication-line wiretapping is of little concern to some computer users, but to others it is vitally important. As previously noted, Petersen and Turn suggest that wiretapping can be "active" or "passive."[40] Physical procedures for controlling wiretapping are discussed in Martin[41] and Harry Katzan.[42]

Finally, electromagnetic radiation and system eavesdropping are accomplished by bugging devices, by cameras, by picking up wastepaper, by visual eavesdropping, and by electronic methods. Martin suggests many controls to minimize these threats from occurring which include isolation of computer centers, shredding of wastepaper, and restricting

entrance to computer centers.[43]

Physical security measures might also be employed to insure the reliability of the computer system. Clearly, it is essential that the computer perform in the manner that it was designed to perform. Any deviation from that performance can result in disastrous security breaches. Reliability has always been an issue to computer manufacturers but it becomes a security problem, as well, if data in the system can be modified or destroyed due to the unreliability of the computer system.

In many cases, generalized rules can be suggested which are adequate for all installations as long as careful consideration of the possible risk associated with each event is clearly understood.

Authorization procedures. As computer systems have grown in complexity, the requirements for efficient operating systems have grown. At the same time, the number of users sharing a computer system and the number of ways in which they use the system have also grown. The operating system is often called upon to grant or deny access to data stored in the system or stored on hardware controlled by the system. Authorization considerations are, perhaps, the most complex problem to be considered in the design of multi-user systems.

The problem is one of restricting access to various

resources of the system based on a "need to know" philosophy. These restrictions, controlled by the operating system, can be placed on: 1) the users of the system, 2) use of terminals or other input/output devices, 3) use of application programs, 4) use of data sets or data elements, and 5) use of selected volumes of the data files.[44]

While most systems have been built on the premise of restricting access to various segments of the system, recent consideration has been given to building the procedures based on privileges to be granted to the user. Therefore, if a user requires certain devices, and/or data, he can access them only if he has the proper privileges. When there are errors in the granting of privileges they are reported quite quickly, while with the other approach, some access errors might never be found.

When access is restricted, the problem of being able to properly identify the user is encountered. The three ways in which a person can be identified are: 1) by some physical personal characteristic, 2) by something he knows or memorizes, and 3) by something he carries.[45] The last two of these procedures can easily be bypassed by other than the authorized user by theft or knowing the same facts, while the first procedure cannot be. In both cases, the probability of a false rejection or a false acceptance must be minimized.

1. Identification systems

Systems that authorize use of the computer system by some personal characteristic are referred to as identification systems. They use finger prints, voice prints, or finger length to positively identify the potential user. More exotic measurements such as head size or lip prints have also been suggested. These procedures have a very low probability of error,[46] and are the most effective. Currently, their use is restricted to military operations and only the most sensitive commercial applications.

Most common of the three identification procedures is identification by something the user knows or memorizes. In the most widely used systems, a user signs on with his user number and a password. If he enters the wrong password he can be shut off the system or given the opportunity to try again. Edward C. Glaser notes that two difficulties are that obvious passwords are used and passwords are stored in obvious places.[47]

To combat these problems some installations issue a new password each month, but this only gives a day or two of protection as the passwords are again put in their obvious places. Bernard Peters has suggested the use of "once-only" codes.[48] With this procedure the user is given a list of codes each month which he uses in order as he signs on. The primary problem with this system is that it requires a large amount of storage space for the password

lists.

Les Earnest proposes that a random number, x, be supplied after the user logs in. On x the user would perform some mental transformation, T, to yield y = T(x). He then inputs y, which the computer certifies. A wiretapper would only have access to x and y, making it nearly impossible to determine T.[49]

Others have suggested that the password be something that the user knows, such as his mother's maiden name. The computer would store a number of facts about the individual and randomly select a fact at sign-on. Like "once-only" codes, this requires a great deal of storage space.

Identification by something carried is the least effective procedure but also the least costly. Usually the item carried is a key, a card much like a credit card, or a badge. A key, of course, would be used to turn on a terminal much like the ignition of a car. Badges and cards are either optically or magnetically encoded and are placed in a terminal to be read.[50] Regardless of the obvious problem that they can be lost or stolen, the use of cards can be expected to grow quite rapidly due to their ease of operation.

2. Authorization techniques

A number of authorization techniques have been suggested which may or may not have been developed with a specific operating system in mind. Some of the most important are based on authority items, authorization tables, access ma-

trices, and Lance Hoffman's "formularies."

D.K. Hsiao suggested and implemented files which contain authority items used to control access to records in the files. His work represents the first working system which controls access at a level lower than the file level.[51]

In Hsiao's system, one authority item is associated with each user. Within the authority item, logical expressions indicate for each file which records are inaccessable, which are temporarily blocked, and which are presently opened for use.[52] In addition, the user can create a procedure associated with a file that he owns to control access by other users. This idea was expanded upon by Hoffman.[53]

Authorization tables have been suggested as procedures for controlling what each user is permitted to do or which give other permissible relationships. They can control access by specifying: 1) transaction types, 2) programs, 3) data sets available for reading, 4) data sets that the user can modify, and 5) data sets in which the user can insert or delete records.[54] The tables have an entry for each user defining what he is entitled to do.

An access matrix is much like an authorization table. The columns represent objects which are entities to which access must be controlled while the rows represent subjects which are active entities whose access to objects

must be controlled.[55] Included in the matrix is a decision rule establishing access relationships between the subjects and objects.

It has been suggested[56] that a number of characteristics of security matrices make it difficult, if not impossible, to implement authorization techniques that employ security matrices. Among those reasons are the following: 1) there are usually more objects than subjects, 2) the matrix is sparse, 3) two or more rows may be identical, 4) two or more columns may be identical, and 5) many matrix entries are identical.

Conway, Maxwell, and Morgan suggest that a practical implementation of the security matrix concept can be successfully accomplished if one or more of three suggestions are employed. First, the size of the matrix might be reduced. Secondly, it might be possible to simplify the entries in the matrix from the general "decision rule" to a binary yes-no indication. Finally, through a careful analysis of when and how the matrix should be interrogated, implementation might be made easier.[57]

Hoffman's "formulary" approach was developed as part of his Ph.D. dissertation at Stanford University. The decision of whether a user can read, write, update, etc., data is controlled by programs (referred to as "formularies") which can be completely independent of the contents or locations of raw data in the data base. The decision to

grant or deny access can be made at data access time, not only at file creation time as has usually been the case in the past.[58]

The basic idea behind the formulary method is that a user, a terminal, and a previously built formulary must be linked together in order for a user to perform information storage, retrieval, and/or manipulative operations.[59] Hoffman's method has a number of desirable characteristics: 1) no arbitrary processing constraint is imposed on data or programs, 2) the method allows control of individual data elements, 3) no extra storage or time is required to describe data which the user does not desire to protect, and 4) the method is machine-independent and independent of file structure.[60] Many of the concepts found in Hoffman's "formulary" approach are being used in the development of newer operating systems.

Authorization procedures in operating systems are an important part of any security package. Without them, or with weak authorization procedures, the value of the complete security package is diminished and can represent one type of integrity violation.

3. Data integrity

Peter Browne tells us that data integrity is the insuring of accuracy and completeness in data files.[61] To insure this accuracy and completeness, all components of the computer system must be working as they were designed

to work, including software and hardware.

The definition of integrity is expanded by Barry R. Borgerson to include two types of possible integrity violations: 1) one process can interfere with another process, and 2) the state of a single process can be erroneously changed without any interference from another process.[62] He includes programs as well as data files in his definition.

It is possible to define integrity by employing the "single failure principle" found in Stephen W. Leibholz and Louis D. Wilson. This principle states that "it should not be possible to lose data through any single failure in the system even though that failure occurs during operation and goes undetected for some period of time."[63] The word "lose" is defined to include any bad thing that can happen to data.

The integrity of the computer system and the data within it are of great concern to developers of operating systems. In the event that the operating system cannot guarantee the integrity of the data and programs, then the computer system is of little value to the user.

Because of these concerns, integrity interfaces with computer security at almost every point.[64] Without integrity, security is inadequate, and without security, integrity is inadequate. Therefore, virtually all discussions about security relate to integrity, and the reverse is true

as well.

4. Examples

Identifying the user, as well as the devices and files that he will be able to use, is generally the domain of the operating system. Much research has been done on the procedures to be used in the development of a secure operating system and also in actually creating a system that works.

It has been suggested that not only must the operating system protect itself, it must provide an authorization function to allow only approved combinations of individual's, programs, and files to be coupled for execution.[65] Because this requirement is not always found in commercially available operating systems, many institutions have found it necessary to attempt to develop their own secure operating system. MULTICS and ADEPT-50 are good examples.

MULTICS (Multiplexed Information and Computing Service)[66] was developed at Massachusetts Institute of Technology. It serves as a case study of protection mechanisms which can permit controlled sharing of information in an on-line, general-purpose, information-storing system. Five principles underlie the protection scheme developed: 1) base the protection mechanisms on permission rather than exclusion, 2) check every access to every object for current authority, 3) design the security system so that the protection mechanisms are not secret, 4) incorporate the principle of least privilege (every program and every pri-

vileged user of the system should operate using the least amount of privilege necessary to complete the job, and 5) design the human interface for naturalness, ease of use, and simplicity.[67]

To insure data protection, MULTICS incorporates G. Scott Graham's rings of protection as the authorization procedure.[68] Essentially, Graham suggests a hierarchical structure for data and programs which requires that data and programs be stored in a hierarchical relationship based on the sensitivity of the data and/or programs.

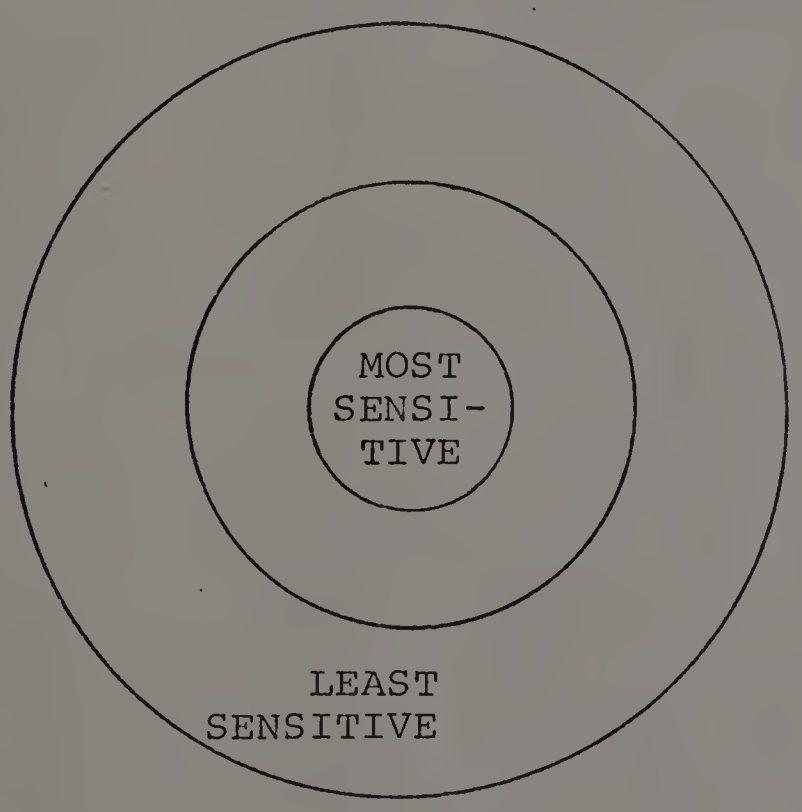


Figure 2-4

Graham's Rings of Protection

All users would have access to the items stored in the outermost ring and only the most privileged users would have access to the innermost ring. Control is at the file level, which has some limitations that will be discussed later.

Surprisingly, access to MULTICS is through a password system. This password system is highly controlled, however, and gives the user the option of changing his password at any time.[69] Should an intruder be able to successfully obtain the user's number and password, he could change the password and prevent the legitimate user from accessing the system. This is a substantial flaw. To counter illegal access attempts, at each login the user is given the time, place, and location of the previous login so that the user is made aware of someone else using his number.[70]

ADEPT-50 is a resource sharing system designed to handle sensitive information in classified government and military facilities.[71] Included in the security objectives of the system are the following: 1) the security control mechanism must support heterogeneous levels and types of classifications, 2) the security control mechanism must be unclassified, 3) the security control mechanism must be constructed so that it might be carefully scrutinized for correctness, completeness, and reliability, and 4) the security control system mechanism be as frugal as possible.[72]

The two major components in the system are security objects and security properties. Security objects are de-

fined as users, terminals, jobs, and files. Each security object is described by a security profile that is an ordered triplet of the security properties, authority, category, and franchise. Authority is a set of hierarchically ordered security justifications. Category is a set of discrete security justifications. Franchise is a set of users licensed with privileged secrutiy jurisdiction.[73]

The security profile is defined in a matrix which has objects in the rows and properties in the columns. Based on the user number, his terminal, his job, and the requested files, the proper security profile is selected and the constraints of that profile govern his level of accessability to the various components of the system.

Encipherment of data. One of the most technical areas in computer security is data encipherment, often referred to as cryptography or privacy transformations. Early work in cryptography was completed far before computers existed so that many of the early developed techniques cannot be easily applied to computer technology. Cryptography is highly specialized and a large body of technical literature has been devoted to the subject.[74] Its presentation here is designed to present an overview of its application to computer technology.

1. Privacy transformations

Turn defines "privacy transformation" as being synonymous with "cryptographic transformation." It was coined

in the early days of computer security research to distinguish the use of cryptographic techniques in civilian and commercial systems from their use for protecting classified national defense information.[75]

Privacy transformations represent one technique for providing data security - the mathematical/logical transformation of the protected data into forms which are unintelligible to all but the holders of the "keys" to the transformations, i.e., those who know what inverse transformations to apply.[76] To employ the techniques of cryptography or privacy transformations we must have a plaintext, a cipher or cryptogram, and a key.[77] The plaintext is the input message while the cipher or cryptogram is the output message. It is necessary to have the key to be able to convert from the cipher or cryptogram back to the plaintext. When the key is missing, cryptanalysis, the art of resolving cipher into their plain texts without having possession of the key, must be employed.

Essentially, there are two main classes of privacy transformations: 1) replacement of characters in the data by other characters (or groups of characters), and 2) transposition of the order of the characters.[78] Another method, compression, is generally not considered a cryptographic technique although its associated confidentiality protection may be sufficient in mild threat environments.[79] Primarily, compression is used to reduce the redundancy in

stored or transmitted data by removing repeated consecutive characters.

2. Hardware

In addition to research on privacy transformations, much work has been done with the development of encipherment ic techniques for terminals. Martin suggests that cryptography at terminals is perhaps more likely to be done by hardware than software.[80] As an example, one manufacturer markets a hardware device for terminals referred to as "Lucifer" which can encipher or decipher messages up to 128 bits in length.[81]

3. Costs

The operation of cryptographic hardware and software is, of course, not without its associated costs of one-time hardware purchase and software development, hardware operation, and degradation resulting from performing the privacy transformation. Of these three, the last is the most difficult to measure. Degradation varies depending on the type of privacy transformation employed. Some measures greatly increase processing time while others only moderately increase processing time. Actual degradation is also dependent on the computer system that it runs on because the internal processing speed of the equipment can alter the effectiveness of the transformation.

Turn reports on work done by William A. Garrison and C.V. Ramamoorthy in which they estimated the increased computer time requirements to be 0.66% for a one-time Verman

ciphering, 3.5% for table look-up Vigenere ciphering, and 6.3% for the modulo arithmetic Vigenere cipher.[82] He points out, however, that these cost figures (obtained on a CDC 6600 computer) are quite sensitive to the type of information retrieval system and that a systematic effort to compile a comprehensive data base of security system costs and decreases in functional capability is clearly needed.[83] Theodore D. Friedman and Hoffman conducted five experiments to measure CPU time on a CDC 6400 required by additive encryption methods programmed both in assembly language and in FORTRAN: a "null transformation" to measure the time to move data without encryption, encryption with a one-word key, encryption with a 125 word key, double key encryption, and encryption using a pseudo-random key.[84] They defined the term "encryption time coefficient" (ETC) as the ratio of encryption time to the time taken to move data without encryption.[85] Their results suggest that transformations coded in FORTRAN will take over twice as long to move the data as will those coded in assembly language (ETC of 9.96 versus 4.21). Increases in CPU time for the routine employed can be expected to range from zero to approximately ten times, depending on the transformation and programming language.[86]

4. Criteria

Dennis Van Tassel suggests a set of criteria for computer-based encipherment systems. It should not be necessary to keep the method secret, only the keys. The amount

of secrecy obtained should be directly related to the amount of computing time necessary to use the system. The method should destroy the statistical parameters or natural structure of the language. Finally, an error should not destroy successive information.[87]

Systems designers must be aware of the suitability of a particular class of privacy transformations so that the system designed does not suffer a great performance loss. This suitability depends on: 1) the relevant characteristics of the particular application, 2) the inherent characteristics of the class of privacy transformations used, and 3) the technical aspects of the system that implements the application and the privacy transformation.[88]

Turn tells us that effectiveness and costs must be weighted against the estimated value of the protected information in order to implement a rational protection system--one that provides a level of data security warranted by the value of the protected information.[89] This might explain why privacy transformations have only found minor use in industry but have been used heavily in military operations.[90]

As the use of network processing expands, and with it the transmitting of more sensitive information over communications lines, we can expect to see the need and use of these techniques grow concurrently. Even today, at least one major application of computer technology requires the

use of privacy transformations. Banks' cash dispensing terminals require that the key be changed after each transaction at the terminal.[91] Otherwise an intruder would only have to tap the line to determine the code for "issue cash" and then he could cause the machine to dispense cash until it was empty. Additional applications can be expected in the future.

Controls. At the heart of any successful security plan is a set of controls to guarantee that the functions mentioned in the preceeding pages are, in fact, in operation and are used to reduce risk in various environments. The use of controls on input/output, processing, hardware, documentation, administrative functions, systems development, and others, is well documented.

Auditors are now paying particular attention to computer operations. As they have become increasingly concerned about control problems in computer operations, auditors have extended their concern to security problems. Obviously, this concern is quite justified if we accept Thomas W. Porter's definition of auditing:[92]

> "Auditing is the examination of information by a third party other than the preparer or the user with the intent of establishing its reliability and the reporting of the results of this examination with the expectation of increasing the usefulness of the information to the user."

To adequately audit a process, auditors cannot stop when the information is put into machine readable form and pick it up

when it's back on paper again. They must be able to insure that these controls are in operation throughout the process.

In addition to the auditors' responsibility, top management must be responsible for the design of the security techniques and procedures and responsible for the day-to-day operations, given that design.[93] To exercise design control, the Bank Administration Institute suggests a number of procedures broken down into administrative controls, system controls, and programming controls.[94] Daily operations should be controlled through operations controls, processing controls, and documentation controls.[95] The responsibilities in these areas can be subdivided among the data-processing manager, the security administrator, local security officers, file owners, line managers, and auditors.[96]

All of these controls should be part of the security plan. Joseph J. Wasserman suggests a hierarchical structure of controls.[97] If the user can answer "yes" to all twelve of his control questions, Wasserman then says that he has a well-controlled system. Others, such as Canning,[98] have also explored the use of controls in security plans.

Miscellaneous Topics

Statistical models. One of the perplexing problems to researchers attempting to prevent privacy threats from

occurring is how they might apply Comber's criteria to the collection and use of data in longitudinal studies and other studies in which the subjects' identity cannot be disclosed. Robert F. Boruch has suggested three strategic models for representing the process of merging records from different sources when confidentiality of the records is required by law or custom.[99]

a. Insulated data bank model. In the first model, the researcher has collected a file of information on n individuals which will be referred to as A with identifiers of I. Therefore, we have a set of n records each containing AI. But, to complete the research, the researcher must use B information from another agency to whom he does not want to reveal A. The AI file is encoded on A to give A'I (where A' is the encoded A) which is given to the agency to merge with their BI file. They return a file of A'B records which are decoded by the researcher to yield a file of AB records. The AB file, without identifiers, can then be used.[100] Many variations of this model exist and Boruch describes some of them.

b. Brokerage model. The brokerage model assumes that the researcher does not want to give his file to the agency for merging. He hires a broker to act as an intermediary. File A'I is given to the broker instead of the agency. The agency encodes file BI on B and gives B'I to the broker. The broker then merges the files and deletes

the identifiers to yield A'B' which goes to the agency for decoding onB. The agency returns file A'B to the researcher for decoding into AB. Although this model is much like the insulated data bank model, the agency has been relieved of the task of merging while the broker works with data that cannot be interrogated by them.[101] Again, Boruch describes a number of variations.

c. Linkage model. The third model is used for logitudinal studies. Assume that the researcher must collect information yearly on a number of subjects, but that in the research their identity must not be known. When the first set of questionnaires is returned three files are created: 1) a data file with unique identifiers, 2) a name and address file with unique identifiers which are different from the data file, and 3) a "link" file in which the identifiers are matched. Boruch suggests that in extreme cases the link file could be stored in a foreign country to prevent it from being subpoenaed.

When a follow-up study must be done, the name and address file is used to produce the address labels for the questionnaires. Upon return, the questionnaires are machine prepared with the second identifier. Then this file is matched against the link file and the identifiers changed. Now the new file, with no reference to name and address, can be used with the original data file.[102] This is essentially the procedure employed by the American Council of Education

in a study of students attending a national sample of colleges and universities in which over a million students were sampled in 1966 and follow-up studies done on approximately 250,000 students.[103]

The collection and use of statistical data remains a problem. More frequently the researcher must demonstrate that his work will not invade the individual's privacy. In many institutions all research projects must be approved by a privacy panel. This trend is likely to continue.

Comprehensive security plans. In the previous pages we have discussed various aspects of security and commented on some of the people working on security problems. Physical security problems have been the concern of such people as Van Tassel and Martin while highly technical software problems are of interest to Hoffman, Turn, Katzan, and others. Reviewing all of these problems are the auditors such as Porter.

The missing link is a comprehensive security plan to put all of the pieces together into something that the user can work with. This need has been perceived by many including Leonard Krauss. His book, SAFE, Security Audit and Field Evaluation,[104] is essentially a set of checklists to be used in setting up a tailor-made security package. Krauss provides the user with ratings to be employed and procedures for interpreting those ratings.

His procedures have been adopted by the accounting firm

of Ernst and Ernst.[105] They provide a "security audit" service in which they analyze a client firm's computer operation and make suggestions for raising the level of security in the operation by reviewing nine potential problem areas.

A similar service is provided by Peat, Marwick, Mitchell[106] which requires an extensive commitment of money and personnel from the client firm. They review ten potential problem areas.

At least one other accounting firm in the "Big Eight," Arthur Andersen, offers a similar service as do several consulting firms.

It should be noted that most of the above are individualized packages developed based on the user's needs. None of the accounting firms sell a "do-it-yourself" package. Only SAFE was built to be used solely by the user without any outside support.

Because of the wide variety of computer uses and the differing threat environments that they are employed in, security plans must be built for the individual. Research and experiences with certain techniques can suggest how they might be used in varying situations, but putting all of the pieces together must be done for each user.

Each user must design his own security plan based on the question "What do I need?" Unfortunately, he must also be able to answer the question, "How do I know when I've got it?"[107] as well. This question is as difficult to re-

spond to as the first, and it is seldom possible to insure that adequate security exists.

Extent of Concern

Users are becoming increasingly concerned about computer security. A well developed security plan covers all of the issues mentioned in the preceding pages and many users are concerned that they don't have adequate security. Their concern increases when events of computer abuse are reported in the trade journals or when they experience them. In this section, we will briefly review the computer abuse problem and then review how this has influenced concern among users and vendors.

Computer abuse. Computer abuse is defined by Donn Parker as "all types of acts distinctly associated with computers or data communications in which victims involuntarily suffer or could have suffered losses, injuries or damage or in which perpetrators receive or could have received gain."[108] Hundreds of examples exist in which programmers, using the computer as a sophisticated tool or white collar crime, had round-offs deposited to their accounts, stole and sold mailing lists, deposited dividend checks to a programmer's account, and made payments to non-existent vendors.

Designed to gather data and report on computer abuse, Parker's study investigated nearly 150 different incidents of computer abuse.[109] While he believes that the gross

amount of crime will grow, Parker is not willing to predict that the loss per incident will increase as a direct result of the increased use of the computer in the financial and industrial community.[110]

Parker found that often the computer played no part, or a trivial part, in the reported computer crime. Also, in at least one-half of the reported crimes, collusion occurred, but he did not find any evidence of involvement by organized crime.[111]

Parker found cases of computer abuse in newspapers which were then verified, if possible, by personal interviews, editorials, newspaper clippings, and legal documents, among other things. Only 68 of the reported 148 cases have, as yet, been verified. This is the first attempt to record in any meaningful manner the results of computer abuse.

Before leaving this topic, we should mention the remarkable case of Equity Funding Corporation, a large California-based insurance company. In April of 1973, it was reported that high officials of the company had used the corporation's computers to create false insurance policies and to inflate the apparent financial status of their company.[112] Approximately 60,000 bogus policies were created in a period of about three years which will eventually result in the loss of nearly $2 billion.[113]

Although this incident is clearly a case of securities swindle, it must also be considered a case of computer abuse

because the computer was used as the principle tool in the swindle. Because of this event, increased interest has been shown in computer auditing and computer security. When participants at a conference on auditing and computer security are asked why they are there, they most frequently make reference to Equity Funding.[114]

For a brief detailed discussion of the Equity Funding swindle the reader is referred to Christopher Podgus' "Outwitting the Computer swindle" in the September, 1973, edition of Computer Decisions. Raymond Dirks, the man who reported the swindle to the New York Insurance Commission, and Leonard Gross have published a book on the subject entitled, The Great Wall Street Scandal. Both are well worth reading.

Vendor concern. Manufacturers have become increasingly aware of their responsibility to provide security to their customers. They are aware that they must offer operating systems with adequate software protection as well as responding to individual customer security needs. Therefore, in 1972, Thomas J. Watson, II, announced that IBM would commit over $40 million to the study of security problems.[115] Part of that investment went to a two-year joint study with three outside users. In July, 1974, IBM published the results of that study.[116]

The Department of Finance of the State of Illinois, participant in the study, published security guidelines for

users. They suggest that management establish what data is being collected, identify who needs it and why, assess an economic value to the data and qualify its worth to outsiders, review the probabilities of disclosure, and budget accordingly for security-related costs.[117]

Another participant, TRW Systems, prepared a list of 187 requirements as a guide in determining whether a system is acceptably secure. The requirements were broken down into five major areas: separation of programs and data, controlled access, identification, surveillance, and hardware and software integrity.[118]

The third member of the group, Massachusetts Institute of Technology, considered the problem of authorization and delegation. Another group at MIT looked at differences in security requirements within the fields of education, health care delivery, financial institutions, and the service bureau industry.[119]

While the project was costly to IBM and involved much research effort at all three locations, the results are not monumental. The final seven volume report appears to be a collection of interesting papers with no string tying the while package together. Apparently little attempt was made by IBM to coordinate the efforts of the three groups and little, if any, direction given to the group members.

Although it appears that IBM derived more public relations from this project than worthwhile research, one must

remember that this was only a small part of the over $40 million that they have committed to computer software and hardware security. In addition, they have trained a large staff of security technicians to work with top management in client companies to make them more aware of security problems and to consider the consequences of security breaches.[120]

The concerns at IBM are being paralleled at other manufacturers and computer service vendors. They too, are concerned with the issues of software and hardware protection, backup and recovery plans, risk assessment, and all of the other security issues. They have not had the public exposure that IBM has had, nor do they have the funds to commit to such a project.

User concern. Concern about security among users has grown. This concern is a function of reported security breaches rather than any planned changes in company security policy.

The need for security has generally been discounted with the explanation, "It can't happen to us." But as fire, flood, theft, or fraud hit neighboring computer facilities, management becomes more concerned about security in their own operations. In the past, concern would ebb until another catastrophe occurred.

Many recent events including the well publicized events at Equity Funding Corporation and Union Dime Savings Bank, have prevented the concern from ebbing as it has previously

done. Because of this publicity, management and auditors are becoming increasingly concerned about the possibility of such events occurring in their organizations. In addition, state and federal governments have been threatening to pass tough privacy legislation which will require more interest in security as well as privacy.

Perhaps, however, for the user the greatest source of information about security has been the trade journals. Their publications have, over the past few years, contained numerous articles about security and how to handle security problems.

In May, 1970, in Datamation, William Bates published an article designed to acquaint business and data processing managers with areas of vulnerability of information systems and to present a security system framework upon which an organization may build and develop to suit its individual needs.[121] Finally, he concluded by saying, "Although I have uncovered no hard evidence that there is widespread management interest in the problem of information system's security, there does appear to be a growing awareness in some organization's management that information system security is a critical area which requires personal concern."[122]

Frequently, Computerworld publishes articles discussing security breaches, industry reports, and expected legislation. Also, nearly all monthly trade journals have two or

three articles on the subject in the course of each year.

Modern Data, in July, 1974, published a computer security survey.[123] Questionnaires were mailed to a random sample of 2,000 EDP managers. Nearly half were dissatisfied with senior management's awareness of the need for computer security, but 77% could not estimate the cost of a computer disruption. If EDP managers are genuinely concerned with security issues, they need to be able to show senior management cost figures to justify increased awareness.

Summary

Computer security is very complex, but includes the mundane issues like physical security and the extremely complex and interesting issues like privacy transformations and authorization procedures. Adding complexity is the fact that the complete set of threats and the complete set of countermeasures are difficult, if not impossible, to determine. Secondly, security remains a very individualized problem. Each user has different security requirements which necessitates that security plans be individually constructed. It is impossible to construct a security framework which would be adequate for large numbers of users.

Finally, interest in security issues is growing at a rapid rate. The vulnerability of the computer system and the data entrusted to it is now becoming an issue that data

processing managers can no longer avoid. The goal of developing a secure system is being pursued by vendors, users, and academicians alike.

Unfortunately, all of the countermeasures attempt to attack a problem which few people totally understand. Security is only an issue if there is something that requires protection. Too frequently there is a lack of understanding about the value of the computer system or its data to the organization. A comprehensive security plan can only be developed when the security needs of the user are clearly defined.

Little research has been done on determining the security needs of the user. Before the security plan can be developed we must determine what requires protection and the extent of the protection required. This can only be accomplished by clearly understanding how the computer is used and the effect that various threats can have on the operation of the organization.

In the next chapter a general framework will be presented for developing a security plan. This framework will allow users to understand where they are going before attempting to get there. Without this understanding computer users are much like Alice when the cat told her that it made little difference which path she took if she didn't know where she wanted to go.

Footnotes

[1]Willis H. Ware, "Security and Privacy: Similarities and Differences," Spring Joint Computer Conference, Vol. 30 (1967), 281.

[2]Arthur R. Miller, The Assult on Privacy: Computers, Data Banks, and Dossiers (Ann Arbor, Mi.: The University of Michigan Press, 1971), p. 204.

[3]Ibid.

[4]Alan F. Westin, Privacy and Freedom (New York: Atheneum, 1967), p. 7.

[5]Peter S. Browne, "Computer Security-A Survey," Database, Vol. 4, No. 3 (Fall, 1972), 1.

[6]Rein Turn, "Privacy Transformations for Databank Systems," National Computer Conference, (1973), 589.

[7]Stewart Madnick, private interview held at M.I.T., Cambridge, Ma., January 22, 1974.

[8]Browne, Ibid., 1.

[9]Ibid.

[10]R.W. Conway, W.L. Maxwell, and H.L. Morgan, "On the Implementation of Security Measures in Information Systems," Communications of the ACM, Vol. 15, No. 4 (April, 1972), 211.

[11]Robert H. Courtney, "A Systematic Approach to Data Security," U.S. National Bureau of Standards Symposium on Privacy and Security in Computer Systems, (March, 1974), 2.

[12]Rein Turn, "Toward Data Security Engineering," The Rand Corporation (P-5142), (January, 1974), 2.

[13]James Martin, Security, Accuracy, and Privacy in Computer Systems (Englewood Cliffs, N.J.: Prentice-Hall, 1973), p. 5.

[14]"Ford Signs Privacy Bill," Computerworld, Vol. 9, No. 2 (January 8, 1975), 1.

[15]Willis H. Ware, "Security and Privacy in Computer Systems," Spring Joint Computer Conference, Vol. 30 (Spring, 1967), 279-282.

[16]Ibid., 281-282.

[17]H.E. Petersen and R. Turn, "System Implication of Information Privacy," Spring Joint Computer Conference, Vol. 30 (Spring, 1967), 291.

[18]Ibid.

[19]Richard G. Canning, "Security of the Computer Center," EDP Analyzer, Vol. 91, No. 12 (December, 1971), 3.

[20]Robert Courtney, private interview held at IBM, White Plains, N.Y., July 22, 1974.

[21]Martin, Ibid., pp. 11-15.

[22]Javier F. Kuong, Computer Security, Auditing and Controls: A Bibliography (Wellesley Hills, Ma.: Management Advisory Publications, 1973), p. 33.

[23]Rein Turn and Norman Z. Shapiro, "Privacy and Security in Databank Systems: Measures of Effectiveness, Costs, and Protector-Intruder Interactions," Fall Joint Computer Conference, Vol. 41, Part I (Fall, 1972), 438.

[24]Robert F. Boruch, "Security of Information Processing-Information Processing-Implications from Social Research," Fall Joint Computer Conference, Vol. 41, Part I (Fall, 1972), 425-426.

[25]Morris H. Hansen, "Insuring Confidentiality of Individual Records in Data Storage and Retrieval for Statistical Purposes," Fall Joint Computer Conference, Vol. 39 (Fall, 1971), 582.

[26]Ibid.

[27]Lance Hoffman, Security and Privacy in Computer Systems (Los Angeles: Melville, 1973), p. 289-293.

[28]Ibid., 290.

[29]Ibid., 291.

[30]Ibid.

[31]Edward V. Comber, "Management of Confidential Information," Fall Joint Computer Conference, Vol. 35 (Fall, 1969), 136.

[32]Petersen and Turn, Ibid., 293-294.

[33]Martin, Ibid.

[34]Ibid., p. 289.

[35]Ibid., p. 291.

[36]Richard G. Canning, "Security of the Computer Center," EDP Analyzer, Vol. 9, No. 12 (December, 1971); Van Tassel, Ibid.; Leonard I. Krauss, SAFE: Security Audit and Field Evaluation (East Brunswick, N.J.: Firebrand, Krauss, and Company, Inc., 1972); and Charles F. Hemphill, Jr., Security for Business and Industry (Homewood, Ill.: Dow-Jones-Irwin, Inc., 1971).

[37]Brandt Allen, "Danger Ahead! Safeguard Your Computer," Harvard Business Review, Vol. 46, No. 6 (November-December, 1968); "Explosion, Fire Destroys Computer, Damage Data Center," Computerworld, Vol. 8, No. 28 (July 10, 1974); "Fire! The Destruction and Rebirth of a Bank Computer Center," Bank Systems and Equipment, October, 1972; Javier F. Kuong, Computer Security, Auditing and Control: Text and Readings (Wellesley Hills, Ma.: Management Advisory Publications, 1974); and Walter M. Strobol, "She Politely Held Door Open-And Admitted "Intruders"-Suggestions for TIghtening Security," Computerworld, Vol. 8, No. 42 (October 16, 1974).

[38]Martin, Ibid., 298-308.

[39]Peter Copeland, private interview held at Milton Bradley Co., Longmeadow, Ma., June 24, 1974.

[40]Petersen and Turn, Ibid., 295.

[41]Martin, Ibid., pp. 334-335.

[42]Harry Katzan, Jr., Computer Data Security (New York: Van Nostrand Reinhold Company, 1973), pp. 77-101.

[43]Martin, Ibid., pp. 342-348.

[44]Martin, Ibid., p. 131.

[45]Ibid., p. 133.

[46]Richard G. Canning, "Data Security in the CDB," EDP Analyzer, Vol. 8, No. 5 (May, 1970), 5.

[47]Lance J. Hoffman, "The Formulary Model for Flexible Privacy and Access Control," Fall Joint Computer Conference, Vol. 39 (Fall, 1971), 92.

[48]Lance J. Hoffman, "Computers and Privacy: A Survey," Computing Surveys, Vol. 1, No. 2 (June, 1969), p. 95.

[49]Ibid.

[50]Martin, Ibid., p. 141.

[51]Hoffman, "The Formulary Model," Ibid., 91.

[52]D.K. Hsiao, D.S. Kerr, and E.J. McCauley, III, A Model for Data Secure Systems (Part I) (Columbus, Ohio: The Ohio State University, 1974), p. 14.

[53]Ibid., 15.

[54]Martin, Ibid., 153.

[55]D.K. Hsiao, D.S. Kerr, and C.T. Nu, Context Protection and Consistent Control in Data Base Systems (Part I) (Columbus, Ohio: The Ohio State University, 1974), p. 1.

[56]Ibid.

[57]R.W. Conway, W.L. Maxwell, and H.L. Morgan, Ibid., 215.

[58]Hoffman, "The Formulary Model," Ibid., 587.

[59]Ibid., 589.

[60]Ibid., 600.

[61]Browne, Ibid., 7.

[62]Barry R. Borgerson, "Dynamic Configuration of System Integrity," Fall Joint Computer Conference, Vol. 41, Part I (Fall, 1972), 90.

[63]Stephen W. Leibholz and Louis D. Wilson, Users' Guide to Computer Crime (Radnor, Pa.: Chilton Book Company, 1974), p. 90.

[64]Browne, Ibid., 2.

[65]AFIPS Systems Review Manual on Security (Montvale, N.J.: AFIPS Press, 1974), p. 45.

[66]A. Bensoussan, C.T. Clingen, and R.C. Daley, "The Multics Virtual Memory: Concepts and Design," Communication of the ACM, Vol. 15, No. 15 (May, 1972), 308.

[67]Jerome H. Saltzer, "Protection and the Control of Information Sharing in Multics," Communication of the ACM, Vol. 17, No. 17 (July, 1974), 389.

[68]F.J. Corbato, H.J. Slatzer, and C.T. Clingen, "Multics-The First Seven Years," Spring Joint Computer Conference, Vol. 40 (Spring, 1972), 579.

[69]Ibid., 573.

[70]Ibid., 574.

[71]C. Weissman, "Security Controls in the ADEPT-50 Time-Sharing System," Fall Joint Computer Conference, Vol. 35 (Fall, 1969), 119.

[72]Ibid., 120-121.

[73]Ibid., 121.

[74]Susan Woolridge, Colin R. Corder, and Claude R. Johnson, Security Standards for Data Processing (London: Macmillan, 1973), p. 176.

[75]Turn, "Privacy Transformations," Ibid., 589.

[76]Ibid.

[77]Dennis Van Tassel, Computer Security Management (Englewood Cliffs, N.J.: Prentice-Hall, 1973), p. 122.

[78]Turn and Shapiro, Ibid., 441.

[79]Turn, "Privacy Transformations," Ibid. 591.

[80]Martin, Ibid., 213.

[81]Ibid.

[82]Turn and Shapiro, Ibid., 443.

[83]Ibid., 445.

[84]Theodore D. Friedman and Lance Hoffman, "Execution Time Requirements for Encipherment Programs," Communication of the ACM, Vol. 17, No. 8 (August, 1974), 445.

[85]Ibid.

[86]Ibid., 449.

[87]Van Tassel, Ibid., p. 129.

[88]Turn, "Privacy Transformations," Ibid., 592.

[89]Ibid., 596.

[90]Martin, Ibid., p. 205.

[91]Courtney, Interview, Ibid.

[92]Thomas W. Porter, EDP Controls and Auditing (Belmont Ca.: Wadsworth Publishing Company, Inc., 1974), p. 2.

[93]Martin, Ibid., p. 351.

[94]"Standards for Internal Bank Auditing in an Electronic Data Processing Environment," Bank Administration Institute, 1972, 13-15.

[95]Computer Control Guidelines (Toronto: The Canadian Institute of Chartered Accountants, 1970), pp. 45-98.

[96]Martin, Ibid., pp. 354-356.

[97]Joseph J. Wasserman, "Plugging the Leaks in Computer Security," Harvard Business Review, Vol. 47, No. 5 (September-October, 1969), 120-121.

[98]Canning, "Security of the Computer Center," Ibid., p. 31.

[99]Robert F. Boruch, "Strategies for Eliciting and Merging Confidential Social Research Data," Policy Science, Vol. 3 (1972), 275.

[100]Ibid., 277.

[101]Ibid., 284-285.

[102]Ibid., 289-300.

[103]Hoffman, Security and Privacy, Ibid., 295.

[104]Krauss, Ibid.

[105]"Computer Security," EDP, Vol. 13, No. 2 (Summer, 1974).

[106] Lee Gagnon, private interview held at Peat, Marwick, Mitchell, Hartford, Conn., August 1, 1974.

[107] Courtney, Interview, Ibid.

[108] Donn B. Parker, Susan Nycum, and Stephen S. Oura, Computer Abuse (Menlo Park, Ca.: Stanford Research Institute, 1973), p. 1.

[109] Ibid., 7.

[110] Ibid.

[111] Richard G. Canning, "Computer Fraud and Embezzlement," EDP Analyzer, Vol. II, No. 9 (September, 1973), 2.

[112] Christopher Podgus, "Outwitting the Computer Swindler," Computer Decisions, Vol. 5, No. 9 (September, 1973), 12.

[113] Parker, Nycum, and Oura, Ibid., p. 3.

[114] Javier F. Kuong, private interview held at Wellesley Hills, Ma., July 12, 1974.

[115] Browne, Ibid., 2.

[116] Tom Alexander, "Waiting for the Great Computer Rip-Off," Fortune, Vol. XC, No. 1 (July, 1974).

[117] "Data Security: What IBM is Doing," DP Dialog, 1974.

[118] Ibid.

[119] "Data Security and Data Processing," IBM Corporation, July, 1974.

[120] Courtney, interview, Ibid.

[121] William S. Bates, "Security of Computer-Based Information Systems," Datamation, (May 1970), 60.

[122] Ibid., 65.

[123] "A Computer Security Survey," Modern Data, Vol. 7, No. 7 (July, 1974), 52.

C H A P T E R III

DEVELOPING A SECURITY PLAN FOR A DATA BASE ENVIRONMENT

A Contemporary View of Data Base Design

Data organization. Data in a data base system is organized quite differently from that found in a traditional environment. In the past, data have always been organized into files created for use by a particular user department. However, data bases create large reservoirs of data that any user can access.

File structures require that a great deal of time be spent in file creation, editing, updating, and sorting of the records in the file. In addition, much time is spent in listing files while little computing is actually done.

When a new need is perceived by the organization, a new file is constructed to meet that need. Generally, new information need not be collected, but information from a variety of other files must be extracted and collected on the new file. This new file is subject to the same problems of updating and editing as the other files.

The data base concept is designed to eliminate the necessity of storing a data element more than once. Also, the use of data bases is meant to reduce the time spent in editing, updating, and sorting of information. In a data base, if an error in the data is found it need only be cor-

rected once rather than at many sources. When information requires updating, it need only be done once. Sorting is reduced by being able to access records on more than one key.

Data bases can reduce the data maintenance time, and offer other benefits to the organization. For example, management can ask questions of the data base and receive responses much quicker than they could before as less complicated programs need to be written to generate these responses. Also, in the traditional approach a request requiring the gathering of data from two or more files might not be accomplished because of time or financial constraints, but with a data base the request can usually be responded to in a reasonable period of time with far less effort by the programming staff.

Employing a data base allows more flexibility in using the available data and provides management with more useful information when they need it. Given their access to more up-to-date information, management will have more timely information to make decisions with.

Key characteristics. To integrate all data that previously was sorted in separate files and to provide management with the ability to satisfy its information needs, the data base must display four key characteristics: 1) common data definition, 2) on-line access capability, 3) effective data administration, and 4) maintenance of security procedures.[1]

Common data definitions are not always necessary in the traditional environment. To one programmer "QUANTITY-ON-HAND" might mean something completely different than to another programmer. In a data base situation, however, "QUANTITY-ON-HAND" will mean the same thing to each programmer and its definition will be clearly established.

Not all systems will have an on-line access capability, but those that don't will have some other means of querying the data base. Often a query language is provided so that a user, on-line or batch, will be able to ask questions of the data base with little or no interaction with the programmer. For example, a user might ask the computer, through the query language, to print the names and addresses of all employees who have an annual income of greater than $50,000 and are divorced. The number of possible questions is unlimited and the effort to produce the responses is far less than in a file structure.

Unfortunately, data elements become outdated and must be eliminated. Others are often added. Existing data elements require updating and editing. In the file environment, the file owner would initiate the requests to make these changes but such a change in a data base environment may effect many more users. Therefore, effective data administration must be accomplished so that the data base is used properly. The position of data base administrator has been established to control access to the data base

and authorize any changes to the data elements.

Finally, security procedures must be maintained. Using a data base means that all data is in one place, which is analogous to putting all of your eggs in one basket. Destruction, or even modification, of that data base could temporarily put the firm out of business. Security procedures in a data base environment are therefore vital to its effectiveness.

Problems. In addition to data organization and the key characteristics of a data base, a number of other problems are encountered when instituting a data base. These include the lack of trained personnel, creation of a need for larger memory banks, greater complexity of reruns, and the difficulty of getting total management commitment to the project.[2]

As data bases have become more popular, the demand for programmers, systems analysts, and data base administrators has grown rapidly. Unfortunately for the data base users, the supply of talented people with data base experience is not as large as the demand. Therefore, training has had to occur in-house with applications programmers re-trained so that they might handle the more difficult data structures found in data bases.

To merge all of the corporation's files into one large data base does reduce redundancy. However, because the data base is used almost continuously, while a file might

have only been used by the system for a short period of time, the memory requirements are necessarily larger. On-line storage is a requirement of data base design.

No matter how well the system is designed, reruns will, at times, be required. Because the information within the data base is constantly changing, re-start checkpoints will have to be made frequently. Transaction logs must be maintained so that the data base can be regenerated should the system go down and the data base is destroyed or modified. Essentially, this is no different from any on-line re-run procedure. However, in a data base more users are affected by a rerun and the types of transactions in the transaction log will be more complex and more numerous.

The creation of a data base requires a great deal of time and effort by the computer staff as well as some large cash expenditures which require a great deal of management support. Management has been conditioned to provide more funds to obtain more reports. But a data base won't produce more reports and, in some instances, it may produce fewer. Its value to management will, at first, be questionable. When the data base comes into existence its users will not be creative or experienced enough to use it to its fullest potential. Commitment will not only be difficult to get initially but it could be difficult to maintain once the data base is in existence.

If one were to ask a group of data base users why they

instituted a data base, the majority would be likely to answer, "To get at data quicker." Data processing managers would probably respond, "To manage data more easily." When the pluses mentioned in the beginning of this chapter are weighed against the minuses just mentioned, it will usually show that a data base can satisfy the needs of both user and manager.

Many of the problems mentioned above can be solved by employing an effective security plan. That plan must be carefully designed to satisfy a number of criteria and must consider the special problems unique to data base systems. In the next section of the chapter factors influencing the design of the security plan will be presented.

Developing a Data Base Security Model

Design criteria. To design a satisfactory security plan, four design criteria must be met: 1) effectiveness, 2) economy, 3) simplicity, and 4) reliability.[3] These criteria are necessary in any type of a security plan regardless if the plan is designed to protect a sophisticated computer system with vast amounts of data stored on-line or if the system is a small batch card system.

To be effective the plan must not allow the data to be modified, destroyed, or disclosed either intentionally or accidentally as it goes into the computer, while it's stored in the computer, or as the data results come from the computer.[4] An effective plan will monitor the operation of the computer system so that it can determine whenever any

of these unfortunate events occur. Simply stated, the computer output should be what was expected from the program.

A plan that was effective in a traditional environment may not be effective in data base environment. In the traditional setting each user had access only to his files, but in the data base his access must be controlled more closely so that he cannot access information that is not in his user domain. To monitor these activities transactions logs must be maintained and access controls instituted.

Given that it is never possible to develop a security plan that offers 100% protection, it is necessary to include economy as one of the criteria. Security needs must be balanced with the funds available. As funds are always a scarce resource that must be shared with other demands of the computer system, economy becomes a very important criterion.

In a data base environment a larger proportion of the funds available for the operation of the computer system must be allocated to security measures. Destruction of a file in a non-data base environment creates a certain amount of inconvenience to the department that the file belongs to, but in the data base environment destruction of a file might temporarily cut off information sources to all departments. While economy is important, system designers must realize that a large proportion of their resources must be committed to the protection of all the data eggs in the one computer

basket.

When we speak of simplicity we mean operating simplicity. For example, if a user at a remote terminal must input his social security number, his mother's birth date, today's date multiplied by three plus two, and a user code, he is quite liable not to use the system because of all the barriers that have been established. It must be remembered that the computer is designed to provide a service to its user and if we make that service difficult to obtain then users will be less likely to fully utilize the computer.

Authorization codes are essential to an on-line data base operation, but to maintain simplicity and security, as well, access to the system's resources has to be controlled by a systems program rather than employing the "twenty questions" approach. Graham's "rings of protection,"[5] Hoffman's "formularies,"[6] or authorization tables[7] are all adequate procedures for most systems.

Simplicity must also extend to the operation of control procedures within the computer center, the tape library, the backup storage facility, and other operational centers. In the event that the control procedures are not simple to operate, employees can be expected to bypass control procedures. Without adequate control, security is a myth.

As for reliability, it is quite evident that the security plan must work continually to be acceptable. The computer system will be of little value if the security plan is

unreliable. Catching some of the intruders some of the time should be unacceptable to security plan developers.

Reliability of the security plan in a data base environment is of particular importance. Failure to catch one intruder could result in disastrous results for all users. In some instances, intrusions might prove to be untraceable although their effect would be felt for a long time.

The relationship between these variables has not been adequately explored. However, it appears obvious that certain tradeoffs must be made to obtain the optimal security plan for the particular institution.

We might hypothesize some of these relationships to aid in understanding possible tradeoffs with security needs. Assume that a firm has determined a minimum reliability that they will accept from the security plan, REL_{min}. Assume, also, that they have determined a minimum response time that they will accept from the system, RES_{min}. Response time can be defined as the minimum time that they are willing to wait at a terminal or the turn around time in a batch environment or some combination of both. In this case, we are using response time as a proxy for simplicity.

The tradeoffs between RES and REL are illustrated in Figure 3-1 along with five different cost curves. Note that the minimum cost that must be expended to obtain RES_{min} and REL_{min} is represented by C_{min} which passes through both RES_{min} and REL_{min}. In this example, C_5 is less than C_1.

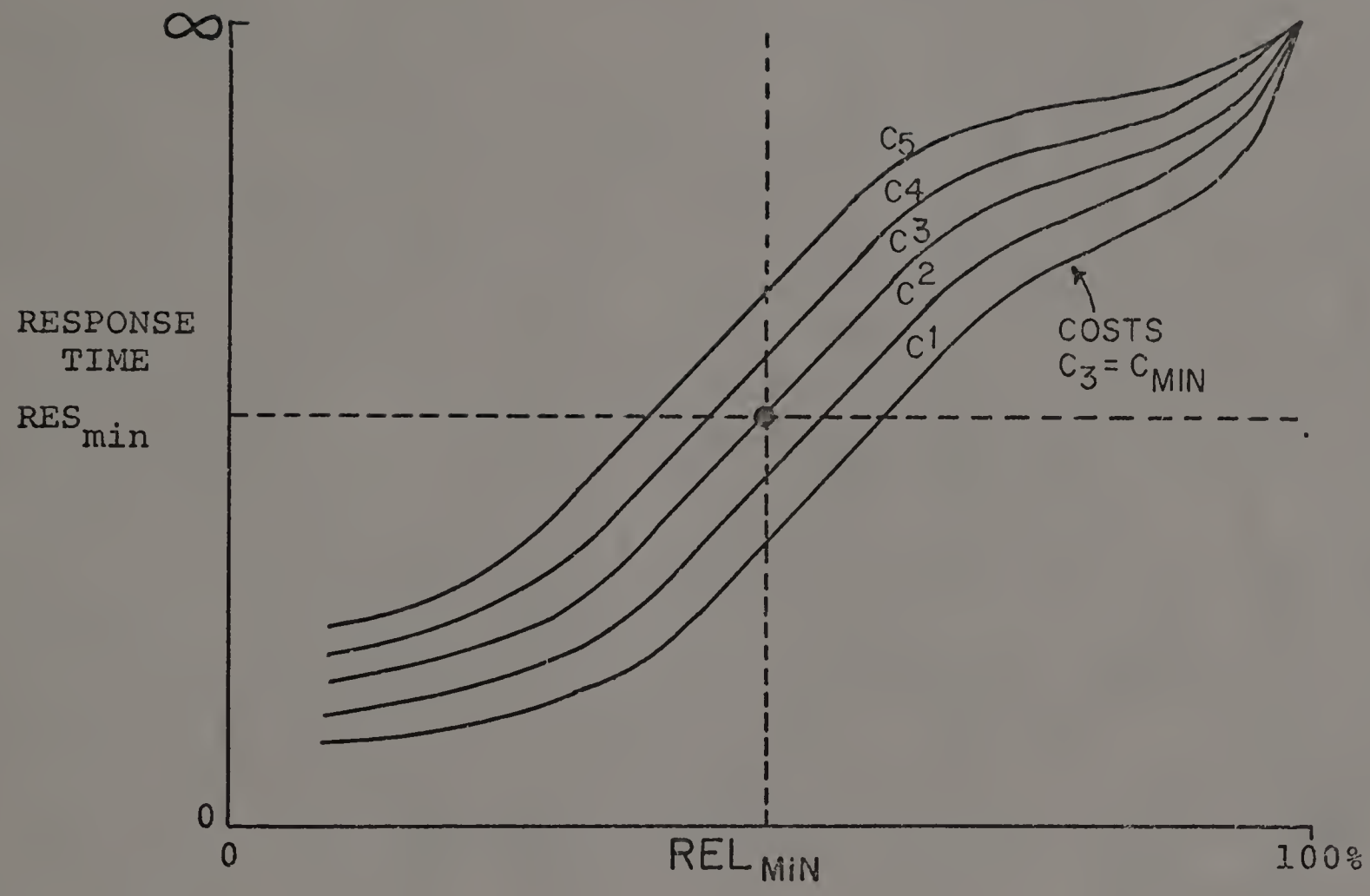


FIGURE 3-1
TRADEOFF BETWEEN RESPONSE TIME AND RELIABILITY

At this same expenditure the firm could increase reliability to approximately 100% but must make a tradeoff with response time approaching infinity. A tradeoff in the opposite direction will reduce reliability and yield a very small response time but obviously never very close to zero.

The shapes of the cost curves are difficult to determine, but their shape in any area other than the southeast quadrant is purely academic because the firm has established the three quadrants as being unfeasible by their selection of REL_{min} and RES_{min}. Tradeoff relationships must be hypothesized only in the southeast quadrant. Therefore, we can only consider tradeoffs when we are talking about security budgets in excess of C_{min}.

As funds are increased two other phenomena can be expected to occur. First, the probability of detecting an intrusion, either accidental or intentional, will increase. Secondly, it is reasonable to believe that intruders will be less likely to attempt an illegal intrusion should they believe that funds are being expended to stop their attack.

In the first case, we suggest a relationship as presented in Figure 3-2. Implications of this figure are that if the firm is willing to devote funds in excess of C_{min} then the probability of detection will increase.

In the second case, we can hypothesize a relationship as expressed in Figure 3-3. This is less obvious than the first case and probably untestable. However, if it is valid, then it might cause the detection line to rise in the previous figure.

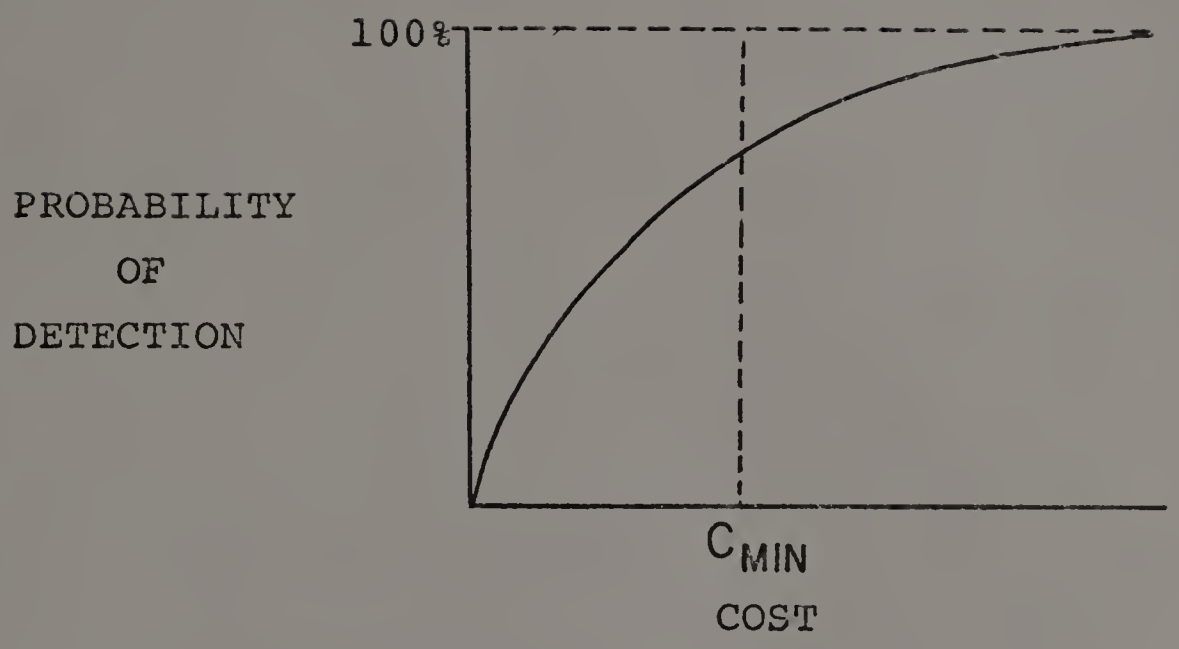


FIGURE 3-2

TRADEOFF BETWEEN PROBABILITY
OF DETECTION AND COST

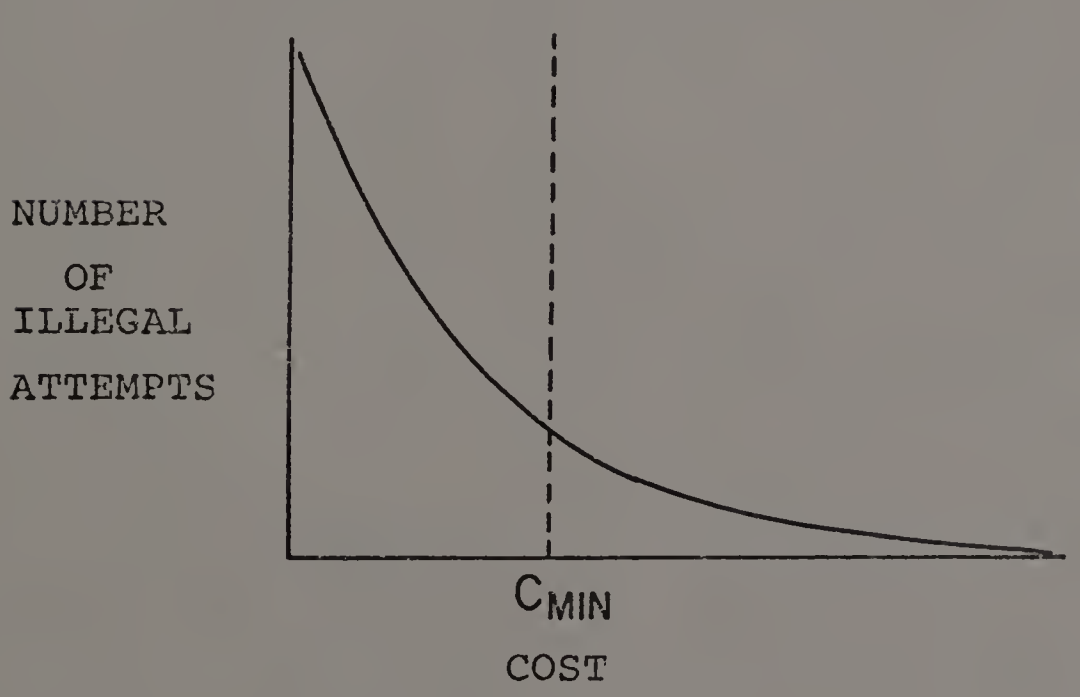


FIGURE 3-3

EFFECT OF INCREASING EXPENDITURES
ON THE NUMBER OF ILLEGAL ATTEMPTS

While the previous discussion is quite hypothetical and cannot, at this time, be shown to be true by measurable data, it does illustrate some of the difficulties in measuring tradeoffs in these criteria. Additional efforts must be made to explore these relationships because of their relationships to security needs and the balance that must be drawn in satisfying these criteria and meeting the security needs of the user.

Objective function. It could even be more difficult to develop an objective function for a security plan. However, some objective function must be established if the plan is to meet the users' security needs. A number of possible objective functions can be suggested.

First, we might suggest that the security plan be designed to maximize the total level of security. Employing this as a possible objective function presents a number of unanswerable questions dealing with measurement and the definition of the term "total level of security." It is difficult to determine when a specified level of security is met. Security cannot be measured in those terms. Often, the only way to measure security is after the fact then it is often found that the security needs of the users were greater than the security level offered by the plan.

A possible objective function could be the minimization of costs. However, if costs are minimized so is reliability and the probability of detection. Using cost minimization

as a possible objective function is, perhaps, the worst possible choice because of its minimizing effects on the other variables. Rather than using it as an objective function, it should be used as an economic constraint in conjunction with another objective function.

A third possible choice would be to minimize potential vulnerability to one user or one user group. In a data base environment this might be the most valuable. Often one user or group of users would be most affected by an intrusion into the data base. Other users are less influenced by problems with the data base and could function, at least temporarily, without the use of the computer which is something that the principle user could not do. It is frequently easy to determine who would be most affected and what vulnerabilities are most likely to occur to their data.

A fourth possible objective function would be to minimize the threat of a particular vulnerability. This vulnerability might be very likely to occur, or the cost to recover, even though it has a low probability of occurrence, might be enormously large. For example, in an airline reservations system if the system is down for a long period of time it would be impossible to make reservations, to cancel reservations, or to know who should be on which plane. It might be possible to develop a security plan which would reduce the probability of this event occurring to near zero.

As regulatory agencies create more regulations about what you can and cannot do with records, the problems of security become more acute. It might, in fact, be necessary to establish an objective function which is defined based on some legal constraints. Credit reporting agencies and banking institutions are governed by laws which determine what type of information can be dispersed and to whom it can be dispersed. The security plan will have to be designed to meet these requirements.

It is not possible to develop one objective function that will satisfy all security plans. Each firm must establish an objective function based on a careful analysis of the security needs of the users. This objective function will provide some direction in the development of the security plan. Without a security objective function the firm will never know when they have acquired the security that meets their needs.

Value of information. One of the most valuable assets of many firms is never seen on the balance sheet. That asset is information. Because accountants are unwilling to include it on the balance sheet, it is often not adequately insured or afforded the other means of protection that would go into protecting a truck or a piece of office equipment. The value of this asset will have a great influence on the amount of security required by the users.

However, the value of the information to the firm is often greater than the cost of many of the firm's assets. When a security plan is instituted that value must be determined but it is often neglected. When this occurs, worthless information is protected dearly and very valuable information is given little protection.

To establish the value of information, three estimations must be made: 1) the value to a potential intruder, 2) the value to the data base owner, and 3) the value to the data subjects if the information is personal information.[8] All three of these must be estimated to determine the degree of protection to be afforded the data base.

In most instances, the data stored on the data base must have some value to an intruder or he wouldn't bother to spend the resources required to obtain the data. It is quite often easy to estimate this value. Can the data be sold? Is it of value to a competitor? Could an employee alter records that might be personally beneficial to him or close associates? These and other similar questions must be looked at and answered fully to determine the value to a potential intruder.

In some cases, value to an intruder cannot be measured in economic terms. We are now in a period in which large numbers of the population have programming expertise. For some of these people, it is a challenge to break the security of the system just for the thrill. This is the most

dangerous intruder to protect against. It is difficult to determine who he is, why he's doing it, or even, when he's doing it.

The value of information to the data base owner can be estimated by determining the effect on the organization were the information lost or disclosed to another source. This can be accomplished by an estimation of the cost to reconstruct the data or an estimation of the potential lost business should a competitor have access to this information. Once this is done the owner of the data base will often find that the information is much more valuable than had been expected. It is at this point that the value of the security plan becomes evident.

The value of the data to the data subjects must also be considered. When confidential data is present on the data base, disclosing the information or altering it incorrectly might cause harm to the individual that cannot be measured in economic terms. In the event that data is not considered confidential, its release might also cause harm to the individual that might not have been considered.

The owner of the data base is often merely a custodian of information required to meet some functional objective. As such, he might be legally liable for damages should the data on a subject be released. In addition to that legal liability, he may wish to consider any moral obligations that he has to protect the data entrusted to him.

Once that the value of all information has been estimated, then this information can be employed in creating the security plan. It is at this stage that certain priorities can be set based on the value of the information and the security needs of the users. For instance, an ordering based on value could be established to determine which data to protect and how much protection to offer it. Also, the information derived in this part of the study can be used to sell management on the need for an effective security plan. In any event, the value of the information stored on the data base must be determined.

Costs of a security plan. Costs relating to the development and operation of a security plan can be broken down into four distinct classes: 1) initial planning and design, 2) initial investment in hardware and software, 3) recurring operation costs, and 4) decreases in functional capability.[9]

To go through the procedures mentioned previously requires a great deal of effort and time. However, by adequately planning and designing a security plan to satisfy all of the firm's need, the firm stands to save a large amount of money in operating costs and future losses resulting from an inadequate security plan.

The planning and design require that representatives of the functional areas have a great amount of input. Therefore, much of the planning and design costs result

from time given up by these people. In addition, large amounts of time and effort are required of analysts and programmers in this phase.

It will quite often be necessary to expand large amounts of funds on investing in additional hardware and software for the security plan to be successful. For example, it might be necessary to acquire an additional tape drive to maintain a transaction log or another terminal to monitor security breaches. Other expenditures might include hardware devices on terminals to prevent unauthorized access or environmental equipment within the computer facility to minimize equipment failure owing to environmental problems.

Increases in software costs result from necessary changes to be made to programs currently in operation. These changes might include additional control totals or different authorization procedures. In addition, the operating system might require upgrading to adequately handle the transaction logs and authorization procedures. In some instances, firms have found it necessary to upgrade from DOS to OS with its corresponding requirements of additional memory and other devices.

Hardware considerations include the requirement for extra backup facilities. These include investments in off-site storage facilities which could include a vault.

A security plan will have associated with it certain recurring operating costs. Included are the operation of the backup storage facility, the regular backing up of the data base, and the purchase of tapes and disk packs to supply the facility. Additionally, regular testing of the plan will be required as well as a periodic review to determine additional requirements or the adequacy of the current plan. These require a committment of time and effort by members of the data processing staff.

Finally, there will be some decrease in the functional capability of the system. Programs will operate slightly slower because of the increased use of authorization procedures and the maintenance of transaction logs. If encipherment techniques are employed they will add an overhead to the operation of the computer facility. These are the most difficult costs to measure and are receiving a great deal of research effort.[10]

Costs must be classified to determine the ultimate benefit of a security plan. Often some of the costs can be directly related to a particular benefit that will accrue from the plan to determine the true value of the particular security procedures suggested. However, in most cases the sum of all of the costs will have to be weighed against the sum of all of the benefits to be derived.

Summary

A security plan for a data base environment is, because of the organization and use of the data base, different than in a traditional setting. In this chapter we have outlined the differences in data organization, the key characteristics of data bases, and have enumerated some of the problems with the use of data bases.

Security plans, for traditional settings or data bases, must be developed with respect to certain design criteria. These criteria have been explained and a number of issues relating to their interdependence have been raised. All of the criteria must merge to produce a security plan which meets some objective function which has as constraints the value of the information stored in the system and the costs of developing such a plan. The interaction of these variables has been discussed.

Little mention has been made of how user security needs fit into this large picture. In the next chapter we will review four alternatives for determining security needs in a typical university setting.

Footnotes

[1]William C. House, Data Base Management (New York: Petrocelli Books, 1974), p. 230.

[2]Ibid.

[3]Rein Turn and Norman Z. Shapiro, "Privacy and Security in Databank Systems - Measures of Effectiveness, Costs, and Protector-Intruder Interaction," Fall Joint Computer Conference, Vol. 41 (Fall, 1972), p. 437.

[4]Robert H. Courtney , "A Systematic Approach to Data Security," U.S. National Bureau of Standards Symposium on Privacy and Security in Computer Systems (March, 1974), p. 28.

[5]Robert M. Graham, "Protection in an Information Processing Utility," Communications of the ACM, Vol. 11, No. 5 (May, 1968), pp. 365-369.

[6]Lance J. Hoffman, "The Formulary Model for Flexible Privacy and Access Controls," Fall Joint Computer Conference, Vol. 39 (Fall, 1971), pp. 587-661.

[7]James Martin, Security, Accuracy and Privacy in Computer Systems (Englewood Cliffs, N.J.: Prentice-Hall, 1973), pp. 159-171.

[8]Turn and Shapiro, Ibid., pp. 439-440.

[9]Ibid., 442.

[10]Ibid., 443.

C H A P T E R IV

DEFINING SECURITY NEEDS

Introduction

The site chosen for reviewing alternative methods of determining security needs was the University of Massachusetts at Amherst. It was selected because they had, in early 1974, committed themselves to a two-year project to institute a data base environment, their proximity to the author, and their willingness to work closely with the author. It might be pointed out that a willingness to work with a researcher in matters of secuity is not often found due to the sensitivity of security problems.

User environment. The University of Massachusetts at Amherst is the largest institution in the Massachusetts state college system with nearly 25,000 graduate and undergraduate students enrolled in 1974. In 1960, the University had fewer than 8,000 students. Because of the tripling of enrollments in less than a 15-year period, a great number of buildings were constructed and the staff was greatly increased to provide the student body with the services that they demanded.

The administrative responsibility for processing the records of the students has also increased at an even faster rate. As an example, the undergraduate Registrar processes over 100,000 grades each semester and the Admissions Office

reviews 20,000 to 25,000 applications each year. It is evident that a sophisticated computer system is required to assist in handling the Registrar's and Admissions' workload as well as the other departments serving the students.

Computer environment. Like many academic institutions, the University of Massachusetts has two computing facilities. One is devoted exclusively to administrative functions while the other is used for research and educational purposes. The administrative computer facility is housed in the principal administration building, Whitmore, and includes an IBM 370/145 and an IBM 360/30.

The other computer system, is a Control Data CYBER 74 and is housed in the Graduate Research Center. Security for research data is a very important issue which should not be overlooked. Destruction of this data can result in the loss of many hours or even years of research. Many of the security measures implemented in the administrative system are also applicable to research data. However, this study is being completed on the administrative computer facilities rather than the research computer facilities. The research and teaching facility will therefore not be discussed further herein.

Administrative computation. When the University first began to process administrative records with the computer in 1962, they were using an IBM 1401. Quickly, they grew into and out of an IBM 1460. An IBM 360/30 was installed in 1967 to replace the IBM 1460 and in 1969 the IBM 370/145 was installed to be used as the principal computer to replace an IBM 360/40 in use for only one year. The IBM 360/30 is still used for input and output operations and for the processing of some small applications.

As the University started to employ data processing, each user controlled his own files. Application programs were written for the user employing his autonomous files. The situation looked much like Figure 4-1.

Fortunately, it was quickly seen that many of the files contained duplicate information. Integrated files were then created for use by more than one user department. This situation is pictured in Figure 4-2.

At the current time high integration exists in the student records area. A master file, referred to as "stats," is structured as an on-line file and contains most of the student records for all existing students. Users can acces, update, or create data records on the file based on permissions granted to the user departments through the computer programs that they are able to use. Certain programs are limited in use to terminals residing in certain physical locations.

R = APPLICATION PROGRAM FOR REGISTRAR

B = APPLICATION PROGRAM FOR BURSAR

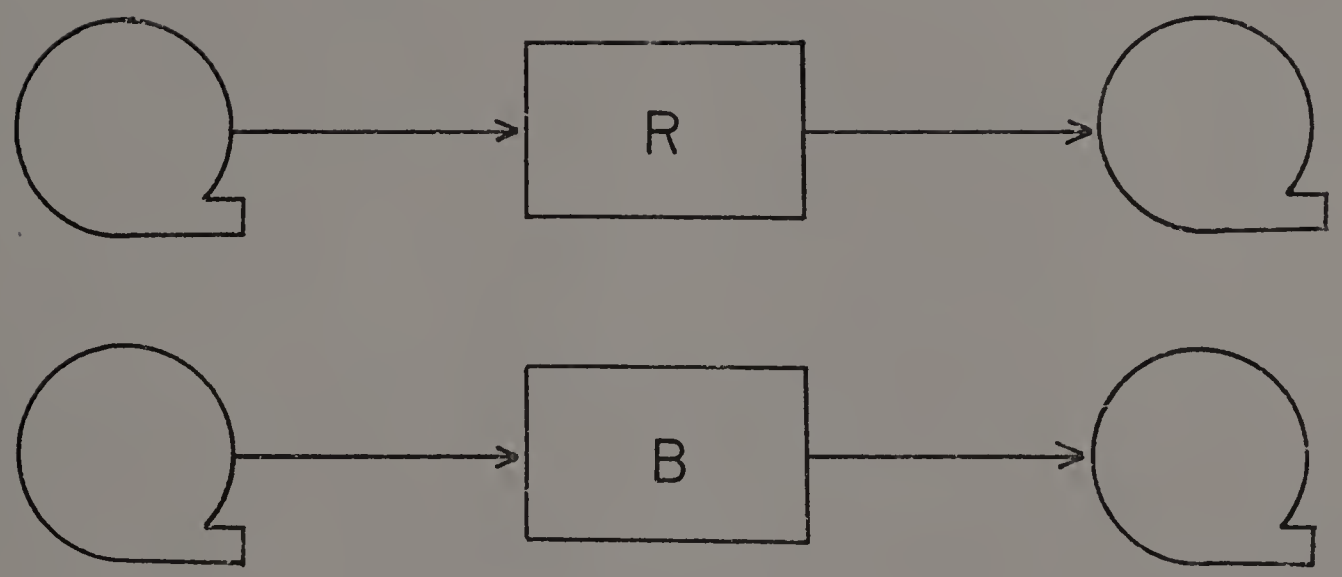


Figure 4-1

Computer Processing Employing Autonomous Files

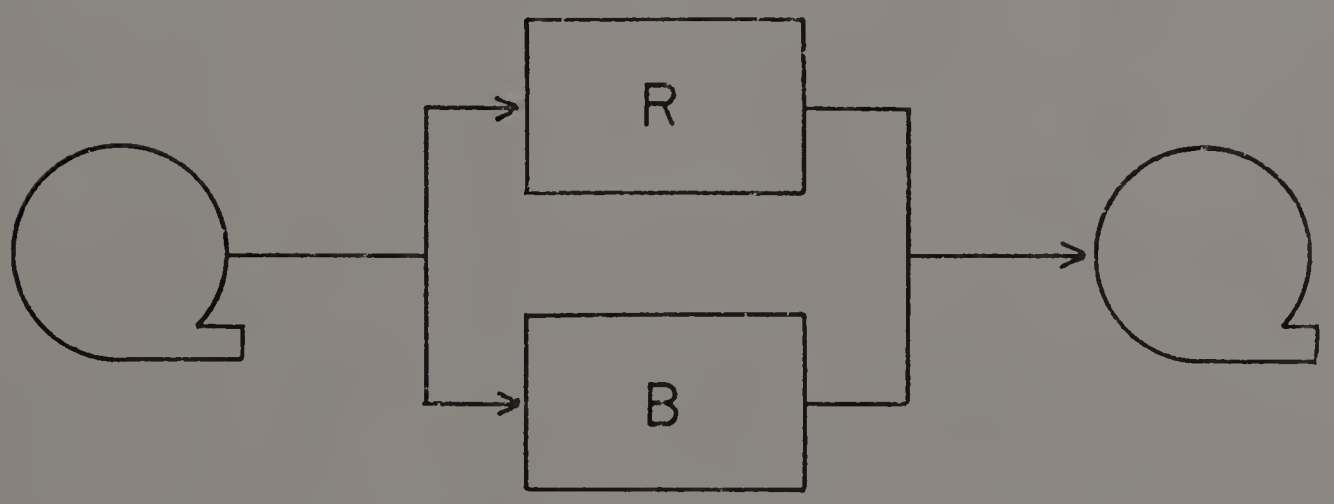


Figure 4-2

Computer Processing Employing Integrated Files

When the data base is installed all functions using student data will use an integrated on-line data base as illustrated in Figure 4-3. Three types of users will exist. First will be those with power to access records only. These users are represented in the bottom of Figure 4-3. They will be required to access the system through an inquiry program which will determine their "need to know."

The second group of users will access the data base directly. These are the principal user departments which are along the right and the left sides of Figure 4-3. Their powers to access, update, or create data records, as well as accessing and modifying computer programs, will be controlled by the data management system.

Finally, ADP and the Data Base Administrator (DBA) constitute the third group. They are responsible for the operation of the student data base. ADP is responsible for the day-to-day physical operation of the data center while the DBA controls access to data elements in the data base, adds and deletes data elements, and has general responsibility to maintain the correctness of the data base.

As of Spring, 1975, the system operates under IBM's Disk Operating System with Virtual Storage (DOS/VS) with hopes of installing IBM's more sophisticated Operating System (OS) by the end of the summer of 1975. The first shift is primarily responsible for servicing 80 terminals throughout the campus that have varying levels of authority

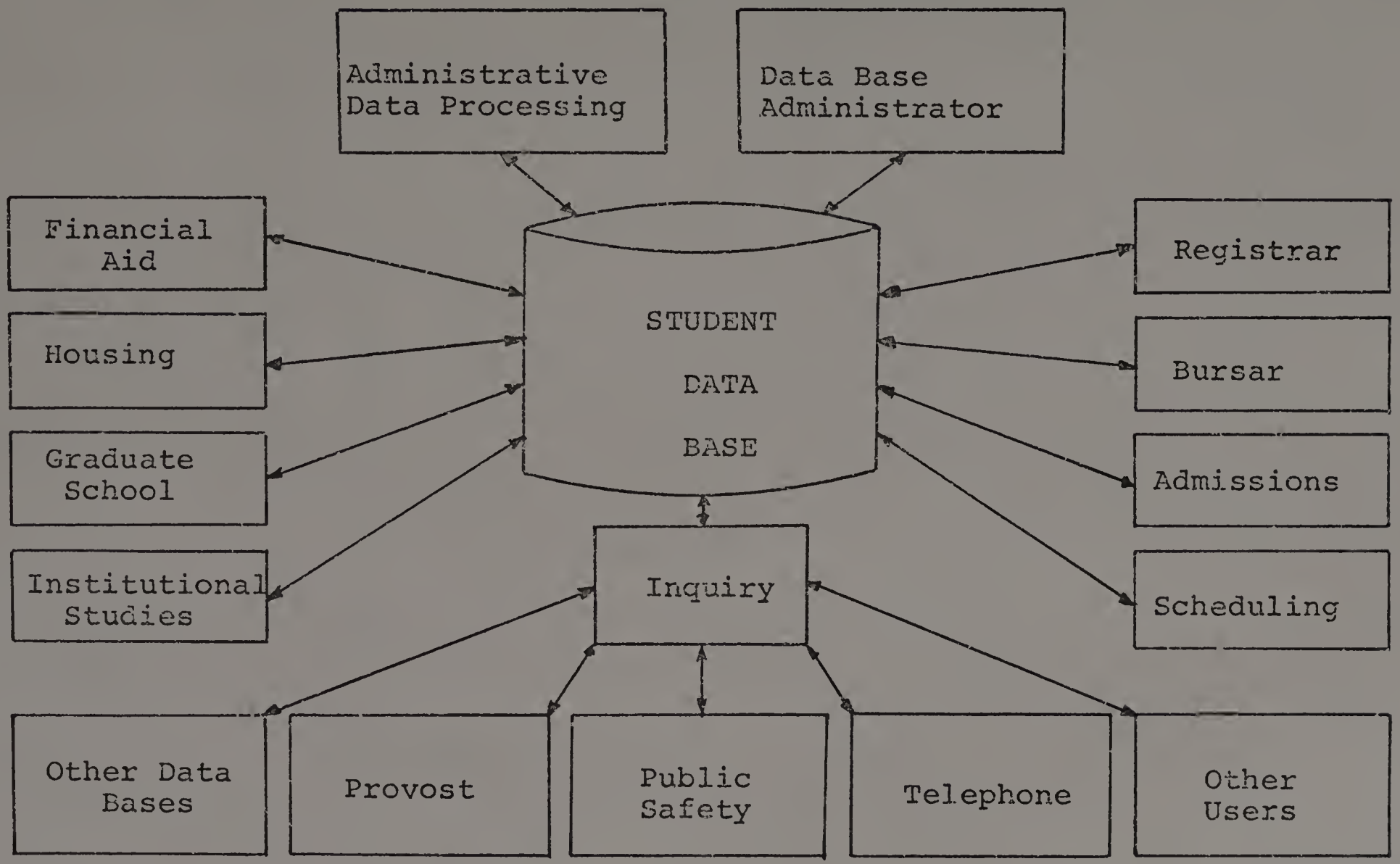


Figure 4-3

Computer Processing of Student Records Employing
A Data Base at the University of Massachusetts

to access and update data records stored on-line. No terminal user has the ability to write or modify computer programs from his terminal. Most production jobs are run on the second and third shifts.

Over 1800 programs exist in the program library. Many of these are AUTOCODER programs written in the middle and late sixties which are still being emulated on both computer systems. In addition, many programs have been patched several times to the point that program changes are often difficult, if not impossible, to make. The use of emulated and patched programs is explained as being necessitated by the rapid increase in demand for computing services which has not been paralleled by similar increases in programming support.

Until January 6, 1975, the computer center operated as an open shop with users being able to wander freely in and out. Since that time, users have been required to submit jobs to be run across a counter and to return to the same location to pick up their output. Only authorized personnel are allowed into the computer center. This change occurred as a result of management's general concern for tighter control rather than a particular problem within the computer center.

The center is located on the first floor of the Whitmore Administration Building. Persons coming down one of the two principal stairways in the building, come upon large windows

which look into the center when they reach the first floor. On the second floor a set of windows allows people to look down on the center from the most travelled corridor in the building which is directly opposite the teller windows in the Bursar's Office.

The physical location, with its large windows, makes the computer center more vulnerable to bombings and take-overs than a less visible computer center would be. In an academic setting, this should be considered as a serious security problem.

Operations of the center are managed by the Administrative Data Processing (ADP) manager. ADP has a staff of approximately 35. The manager reports to the Director of Computer Operations who also controls the operations of the Graduate Research computing center and reports to the Chancellor of the Amherst campus.

Programming and systems development are handled by a staff of approximately 31 in Management Systems (MS). The Director of MS reports to the Director of Budgeting and Institutional Studies who, in turn, reports to the President of the University. It is interesting to note that there is no common reporting point for ADP and MS until they reach the President's Office.

In addition, the Users Advisory Committee, made up of representatives of the user groups on campus, meets regularly to review and make recommendations on the use and

operation of the two computer centers. This committee has recently been expanded to include representatives of the University of Massachusetts Medical School and the University of Massachusetts at Boston. The reason for this action is that the Amherst computing facilities, both research and administrative, will be increasing their services to these campuses.

Due to large increases in user demands for services and great overlaps in information needs of the users, the Users Advisory Committee decided in early 1974 to institute a data base environment. It was decided that five data bases would be established: 1) student, 2) personnel, 3) physical facilities, 4) course, and 5) finance. Management Systems was given two years in which to plan and implement the project. It was further decided that the student data base should be the first to be implemented.

Among the responsibilities of MS during this period of time included: 1) the hiring of a data base administrator, 2) reviewing available data base management systems, 3) determining additional security needs, and 4) installing OS and, perhaps, an IBM 370/158 to replace the 145. Planning for implementation required the employment of critical path analysis which is being followed closely.

Preliminary Investigation

University data bases. As previously mentioned, the

data base system to be established will operate on five individual data bases. As the data bases serve the same community, there will be some variables which will link the data bases together. In addition, some of the elements in one data base might be highly dependent on each other. The relationship of the five data bases is shown in Figure 4-4.

The attention of this study is focused on the first data base to be installed, the student data base. Information stored on this data base will include but will not be restricted to basic identification data, admissions data, housing data, billing data, and academic data.

The course data base is used to establish the scheduling of students into the courses offered by the University. There is a direct relationship between these two data bases during the scheduling period. During this period the course data base will require accessing of various identification and academic data (from the student data base) for scheduling purposes.

All personnel data will be stored on the personnel data base. As many students are employed through work-study programs, the student data base has to be closely related to the personnel data base. Identification data as well as some academic data could be called from the student data base for use by the personnel data base.

Physical facilities will contain information on the buildings and equipment on campus. It will be used to main-

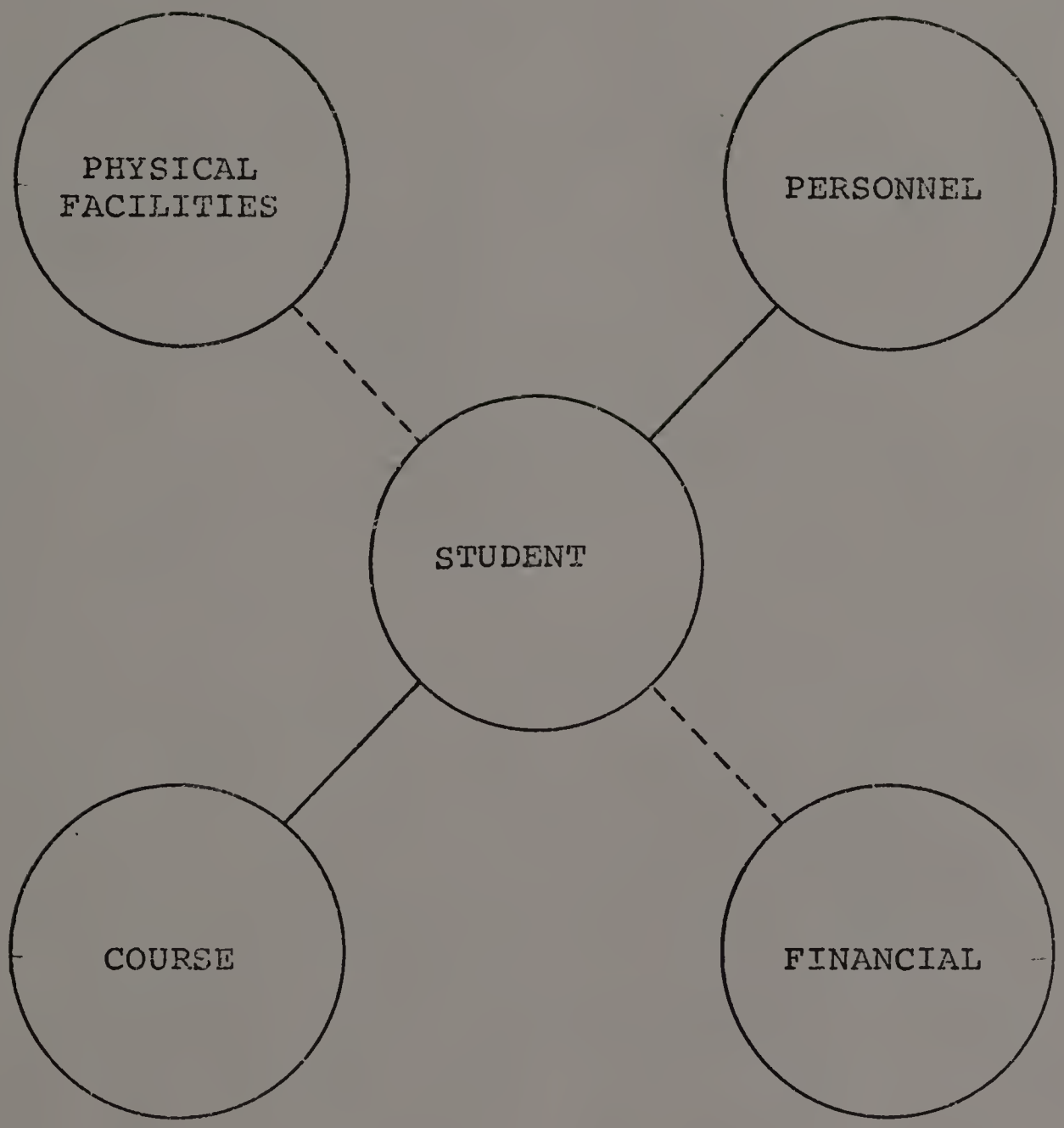


FIGURE 4-4

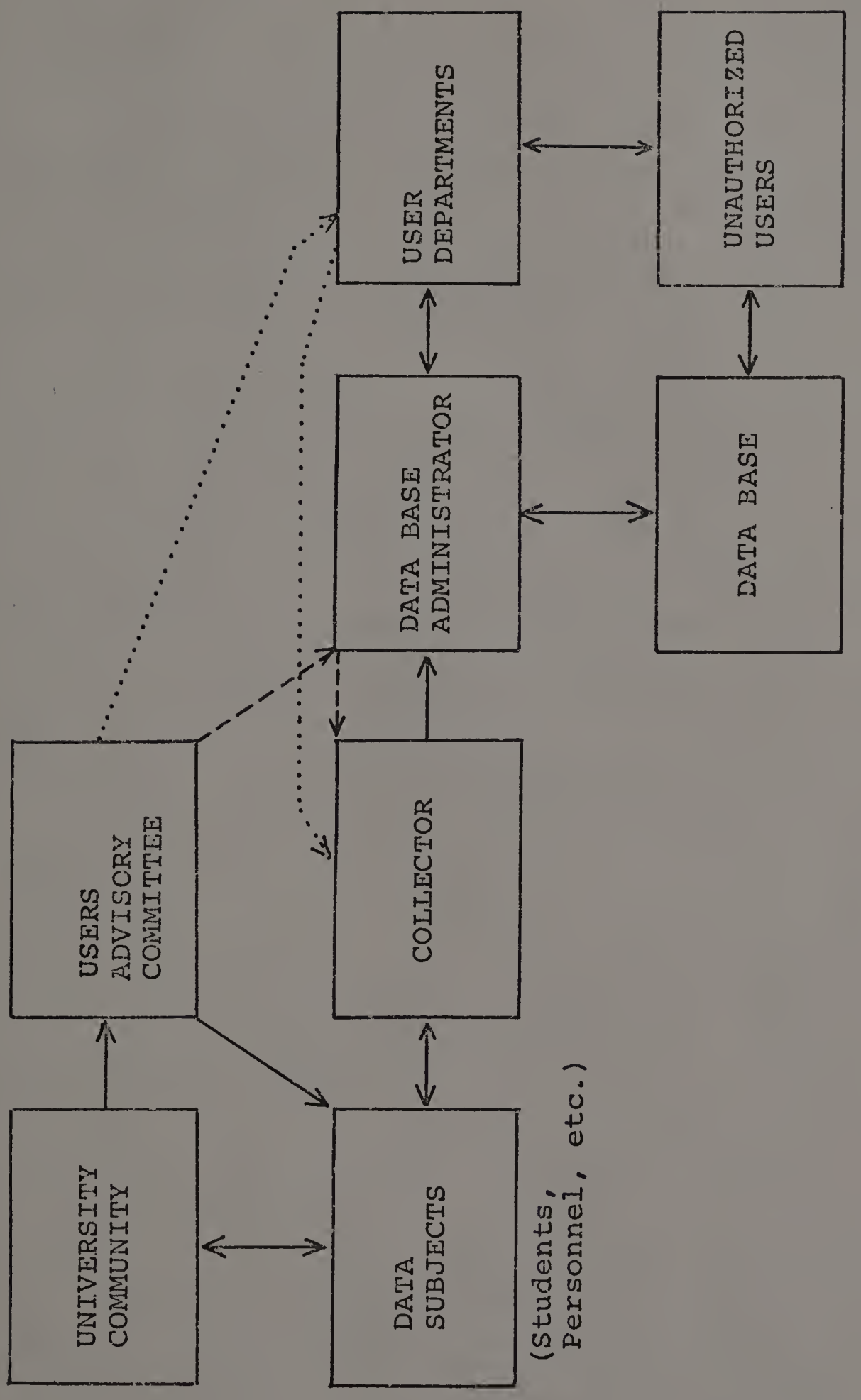
University Data Bases

tain maintenance programs and to coordinate the purchase of supplies and equipment. The relationship between this data base and the student data base is very minor.

Finally, the financial data base is, perhaps, the most important data base to the University in terms of security. All financial transactions will be processed through this data base. Trust funds or other funds controlled by the University could be misused if the computer were used as a tool for stealing. The student data base is only marginally related to the financial data base via billing data.

Although each of these data bases have its own unique security problems, many of the issues involved in one are applicable to another. Therefore, when a similar security problem is solved in one it might no longer be a problem for the others. Given this situation, many of the issues solved in the implementation of the student data base will provide answers to similar situations in the implementation of the other data bases.

Information system structure. An information system cannot be thought of as only hardware and data. It is made up of many other components. All of these components must work together if the information system is expected to function properly. Control of these components is very important--even more so than in a traditional setting. An illustration showing the various components of the data base information system is shown in Figure 4-5.



------ Users Advisory Committee as Controller of Data Elements

..... User Departments as Controllers of Data Elements

FIGURE 4-5

Components of the Data Base Information System

First, the system is established to serve the information needs of some group which, in this case, is the University community. But the University community only exists to satisfy the needs of the data subjects. As the data subjects demand more services from the University community, more information must be collected.

The Users Advisory Committee is a supervisory group which can be thought of as the information controller. They act as an agent of the University community and are responsible for making sure that the information needs are met and that adequate control is maintained on the information.

Within the information system are three other important parts. The collector is responsible for retrieving information from the data subjects. User departments use the information collected by the collector to satisfy their functional objectives. In some instances, the collector and the user departments are one and the same.

Acting as an agent of the user group is the data base administrator. It is his responsibility to gather the information from the collector and deposit it in the data base. He must act on requests from user departments to access, update, or create data elements.

Unfortunately, unauthorized users might want to access the data base. They can infiltrate the data in one of two ways. First, they can obtain data from a user department. This can be with the aid of the user department or through

some illegal means. Secondly, they can illegally retrieve information directly from the system by stealing a data tape, wiretapping or some other illegal infiltration.

The security system must be designed to minimize the second type of data theft. However, the first type is less easily dealt with. It is necessary that the user departments be made aware of the risk of data theft and that they institute actions in their departments to control security problems.

Control philosophy. Control of information in the data base is different than that of the traditional environment. Clearly, the user department was the creator and user of the data file. They were then classified as the file owner and were allowed to control access to the files. As a data base is the consolidation of the files, control must be different than if files are used independent of each other.

The Users Advisory Committee (UAC) responds to the information needs of the University community. Therefore, they are responsible to the University community for the operation of the information system. If they allow the control of the data base to pass to the user departments, then the user departments must establish individual policies for controlling the data elements or must interpret policies handed down by the UAC.

As one alternative the user department would interact

with the Data Base Administrator (DBA) and act as a channel for passing information back up to the UAC. Also, the user department would control the collection of the information for use in the data base. Note, also, that in this situation there is more than one controller of data elements in the data base.

A second alternative would be to have the Users Advisory Committee control the data base. When the Users Advisory Committee controls the data elements we would recommend that they should establish a set of policies and procedures based on the needs of the user departments to be administered by their agent, the DBA. Then control would be through just one source rather than many, as would be the case if the user departments controlled the data elements.

Control of the data element should be exercised at the Users Advisory Committee level rather than at the user department level. The DBA should act as their agent with the following responsibilities:

1. to carry out policies and procedures established by the UAC;
2. to act on user request for new uses of the data;
3. to arbitrate conflicts between users with respect to the use of the data base; and
4. to monitor for security breaches and initiate corrective action.

As an agent of the Users Advisory Committee, the Data Base Administrator will report when policies and procedures

are inadequate, user requests for data cannot be resolved, conflicts cannot be resolved, and security breaches are unusual or not easily resolved. If control is in the hands of the user departments it is quite likely that many, if not most, of the problems that the DBA would handle could filter up to the UAC which would create much extra work for that committee. Also, under the suggested policy the user departments would not have to deal with the time-consuming problems of creating and interpreting policies relating to use of the data or of doing any of the other tasks that the DBA could easily do for them.

When control is solely in the hand of the user departments, the possibility of security breaches is greatly increased. An unauthorized user could request information from various authorized users and, by taking advantage of the different ways in which these users interpret the operational policies, obtain some privileged information that he could not have received by going through the DBA. A situation similar to this could put the University in violation of a federal law such as the privacy bill signed by President Ford on December 27, 1974.

The following guidelines could be instituted:

1. The Data Base Administrator will act as an agent of the Users Advisory Committee and they will have ultimate control over the use of the data elements.

2. The UAC will establish policies and procedures, based on the user department needs, for the DBA to use as guidelines in carrying out the assigned functions.

3. All conflicts concerning the use of the data elements will be arbitrated by the DBA with the user departments having the privilege to appeal to the UAC.

4. The DBA will report periodically to the UAC with respect to new uses of the data elements, abandoned uses of the data elements, results of conflicts and pending conflicts, and other matters related to the effective operation of the data base.

5. The UAC will review periodically the functions of the DBA to determine that their policies are being carried out and that the user department needs are being satisfied.

The suggested procedure would put the control of the data elements in the hands of the Users Advisory Committee who would act based on the needs of the users. The user departments would be freed from dealing with problems of access control to devote their entire energies to servicing the University. This is the only acceptable procedure that can be instituted to give the control necessary to properly operate the data base.

Invisible intruders. It is assumed that user departments mentioned in the previous section will make requests for information from the data base administrator independently of each other. His approval of those requests would be based on their "need to know."

On occasion users could request information jointly from the data base administrator. Again he would act on the

basis of the users' "need to know."

It is the responsibility of the user departments to control the flow of information after it arrives in their departments. They must act in a similar manner when other users request information from them. In addition, print-outs, cards, tapes, and other forms of computer input/output must be controled by them in the same manner that they would control their own files.

However, an intruder could use the good graces of two or more user departments and their respective access to information through the data base administrator to obtain information that he could not have otherwise accessed.

Assume, for example, that the intruder wanted to obtain a listing of the names of all University employees and their annual pay but that this information is classified. If the intruder is employed by some other user department or is a respected member of the University community, he might have no trouble in obtaining this information.

By making a legitimate request to User A (see Figure 4-6) he might obtain a listing of employee names along with employee numbers. This could be a request that the user is quite willing to fulfill based on his perception of the intruder's information needs.

Without knowing about the information that User A gave to the intruder, User B receives a request for a listing of employee numbers and corresponding annual salaries from the

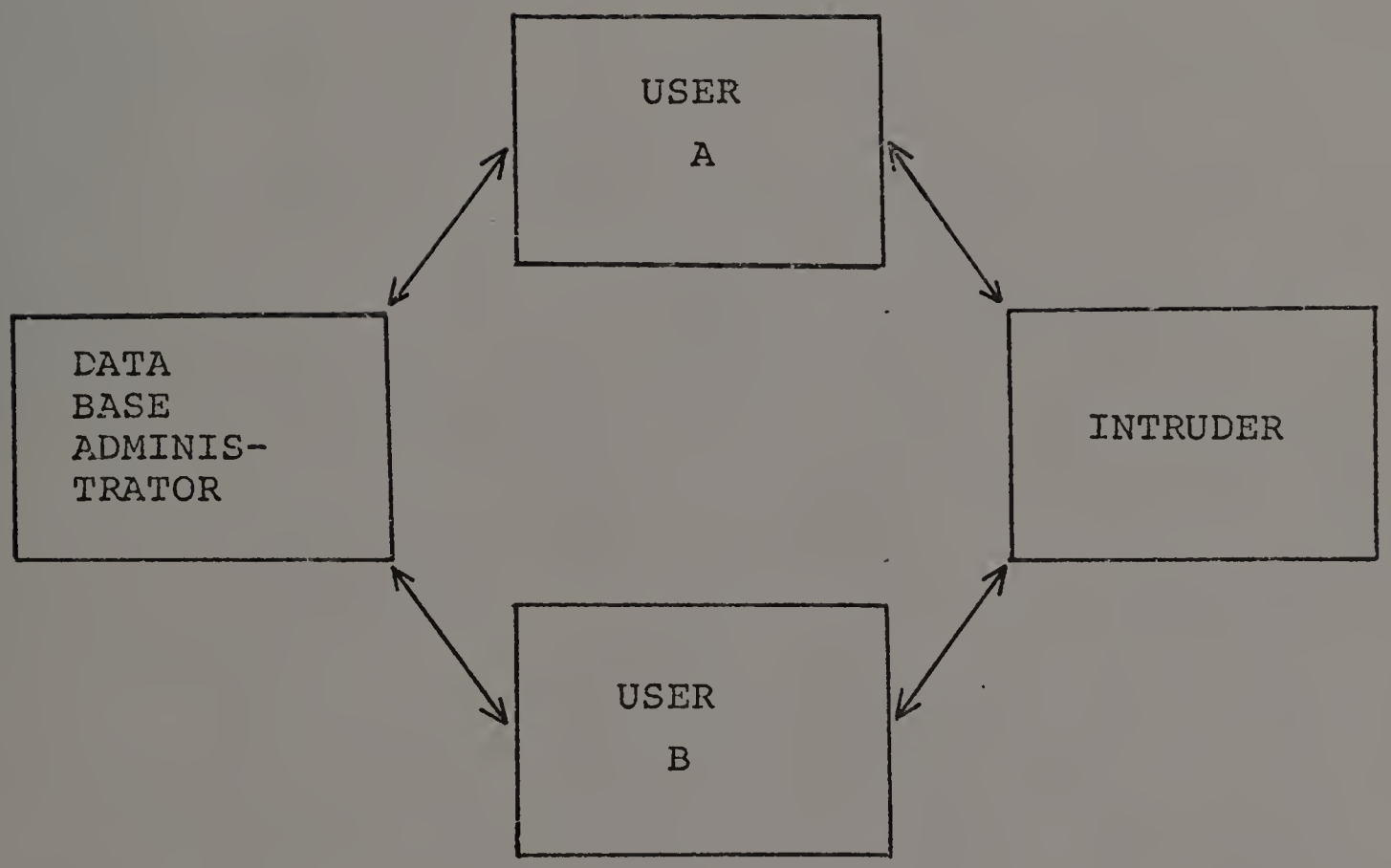


FIGURE 4-6

Invisible Intruders

intruder. As User B believes that the intruder is well within his rights to have this information, he supplies it without question.

Now the intruder combines the two unimportant lists of data and has a list of extreme value. Neither user is aware of any wrongdoing and yet probably has no idea how the intruder got this information.

It is difficult for at least two reasons to protect against this form of intrusion. First, employees are usually willing to supply information to colleagues should they believe that the information will aid the colleagues in their work. Second, it is often difficult to predict when two sets of innocuous data can be combined to produce sensitive information. For these reasons, few, if any, particular countermeasures are available to thwart these threats.

Four methods of analysis. Now that the planned data base system at the University has been fully explained we will look at four methods for determining user security needs. These four alternatives are based on four assumptions which follow.

First, it is assumed that security needs are based on the effect that a security breach could have on a user department. Further, it is assumed that representatives of the departments should be good estimators of those needs.

Second, the actual structure of the data base and the

users' ability to access, update, or create data records are assumed to be the determining factors in the second alternative. This assumes that this information is easily collectable.

Third, data element usage is assumed to be a determining factor of security needs in the third situation. From this assumption we implicitly determine that the most frequently used data elements should be the most closely guarded.

Finally, computer usage is assumed to be the determining factor in the fourth situation. It is assumed that the more a user uses the system the more important his security needs are.

From these four assumptions, four methods of determining security needs are suggested. First, user interviews could be conducted to determine the effect of a security breach on the user departments. The second method could be to examine the structure of the data base by examining the users' ability to access, update, or create data records. A third method suggested by these assumptions, is to examine the frequency with which data elements are used. Finally, the last method examines the actual intensity with which each user uses the computer system.

These four methods were selected because they suggest procedures in which data can be collected in a relatively simple manner for an orderly analysis of the determining

factors of security needs. Should all, or any one of them, prove to be significant in the definition of security needs, then an easily employed procedure for defining security needs will have been revealed.

The First Method: User Interviews

Because a computer system is developed to serve the information needs of the users, it is not unlikely that we should expect them to have some idea about their own security needs. It is assumed that they could measure the effect of being without the system for any period of time and that they could estimate the criticality of the computer operation to their departments.

The major users of the current system are expected to be the major users of the new data base. A list of those users was prepared by Management Systems along with the person most familiar with computer operations in that user department.

Thirteen user departments were identified of which ten were selected for extensive interviewing. Two of the three departments that were not interviewed, Public Safety and Telephone Information, were not interviewed because of their use of data elements in the data base and their inability to create or update records. The other, Stockbridge, controls very few records on the system and has functions identical to the Registrar.

Table 4-1 lists the ten departments that were interviewed. The purpose of each department and a description of its computer usage appears in Appendix A. Also, for those departments that were interviewed, the people participating in the interviews are listed.

Interview process. In eight of the ten interviews the primary objective was the same: to find out more about how the user department used the computer in its operations and to ascertain how various security breaches would affect those operations. Interviews at Administrative Data Processing (ADP) and the Provost's Office did not have the same purpose.

Table 4-1

User Departments Interviewed

Registrar
Bursar
Financial Aid
Graduate School
Provost's Office
Housing
Scheduling
Administrative Data Processing (ADP)
Institutional Studies
Admissions

The interview at ADP was designed to determine what security measures were currently in existence and to determine if the other user departments had left any glaring holes in their obvious security needs. Similarly, the

Provost's Office, where most users report, was interviewed to determine if the user departments over-emphasized their needs and to put all of the interviews into proper perspective.

All of the interviews, including those at ADP and the Provost's Office, were open ended. A series of questions was prepared before the interview but responses to those questions often resulted in other questions being asked. In most departments only one interview took place, but in the Registrar's Office and ADP two interviews were necessary.

Interviewees were asked to estimate the effect on their departments were various pieces of data disclosed, modified, or destroyed. They did this for normal operating periods and for peak operating periods. This information was later used in the development of consequence estimates which will be discussed later.

They were also asked questions relating to the frequency with which they use the computer system, the form of access that they used, their dependence on data supplied by other parties, operational controls in their own department, and various other questions. These are all non-quantifiable responses which must be ascertained to get a good feel of user security needs.

Consequence estimates. Based on the user interviews consequence estimates were prepared. These estimates appear

in Table 4-2.

Users were asked to estimate the effect of not having access to the computer would have on the operation of their departments. They also estimated how long the system could be "down" before serious operational problems would develop in their departments. These estimates were made for both peak and non-peak periods.

During non-peak operating periods two users could get along without computing services for as long as one month. Scheduling could put off most of their computer work until the computer was "up" again. Housing makes infrequent inquiries during this period which could also wait.

Other users were able to do without the system for one to two weeks with the exception of the Registrar who required that the system be brought "up" within one day. Their processing is quite heavy throughout the year and a system failure that extended for any length of time would greatly affect their operation.

Even during non-peak periods system failures have some operational effect on users. The Registrar, Admissions, and the Graduate School would all experience moderate inconveniences while the other departments would be expected to experience only a low level of inconvenience.

During peak operating periods the effect of the system being "down" is, as expected, greatly increased. Even during these periods Admissions, Scheduling, and Institutional

Table 4-2

Consequence Estimates

	Peak Periods		Non-Peak Periods	
	Operational Effect	Time Constraint	Operational Effect	Time Constraint
Registrar	High	30 Minutes	Moderate	1 Day
Admissions	High	1 Week	Low	2 Weeks
Graduate School	High	1 Day	Moderate	1 Week
Bursar	High	1 Day	Moderate	1 Week
Housing	High	1 Day	Low	1 Month
Financial Aid	Moderate	1 Day	Low	1 Week
Scheduling	Low	1 Week	Low	1 Month
Institutional Studies	Low	1 Week	Low	2 Weeks

Studies can be without the system for a period of up to one week. Most other users are crippled after one day but the Registrar can only be without the system for thirty minutes.

In all but three cases the operational effect is high during peak periods. Financial Aid would experience a moderate effect and Scheduling and Institutional Studies both can be rated as low.

As previously mentioned, this table was prepared from user interviews. If however, the responses to questions asked in each interview, without respect to some relative relationship of the users, all users would rate their own inconvenience as high. The interview that was held with the Provost's Office enabled the researcher to put the responses into proper perspective and understand better the effect that such a failure would have on each user department.

It is clear from this table that the operation of the Registrar's Office is critical during both peak and non-peak periods. Even if a failure occurs during a non-peak period for the Registrar that happens to be a peak period for some of the other users, the consequences of such a problem to them is at least as important as to the other users. Implications of this analysis are that a security plan must be developed which will consider the Registrar as the most affected user during all periods.

Peak usage periods. Table 4-3 illustrates the periods

Table 4-3

Perceived Peak Usage Periods

	J	F	M	A	M	J	J	A	S	O	N	D
Registrar	X	X			X				X			
Admissions	X	X										X
Graduate School									X			
Bursar	X	X				X	X		X	X		X
Housing	X								X			
Financial Aid				X	X	X	X	X	X			X
Scheduling										X		
Institutional Studies	X								X			

defined by the users as peak usage periods during the interviews. These periods are important to the users because of the severe operating effect that would result should the system be down during these periods.

It is important to note that this table was developed from perceptions rather than any figures on business activity in their departments. While perceptions are not always accurate, they were drawn from individuals most familiar with operations in their department. In lieu of business activity statistics, they should represent the most reliable information source.

From this table we note that six of eight users identify September as a peak period. Also, five users choose January. No users find March and November to be peak usage

periods and April and August were only selected by one user which happens to be the same user.

Clearly, some months are much more important in terms of the computer's effect on the operation of the University. This table illustrates the user's perceptions of those periods.

A user's perception of his information needs could have some bearing on his security needs. The interviews, however, did not shed much light on the relation of information needs to security needs.

Users were unwilling or unable to conceive of many of the possible security breaches that were discussed. As a group, they were willing to abdicate this concern to ADP and MS if, in fact, they thought it to be a concern. No user had even given consideration to a contingency disaster plan. Little concern was given to the possible modification or disclosure of data.

The interview process is important because of its value in learning how the user departments use the computer. This first method also provided information relating to the peak usage periods and the consequences of system failures.

Insights established from this process are not as valuable to defining security needs in the selected setting as we would have liked to have seen. It is not possible to conclude that any general framework for the establishment of security needs can be established from this interview

process.

One can conclude, however, that awareness of security problems is lacking. Perhaps if the users were more aware of security problems and the implications for the operation of their own departments, then the interview process would be more beneficial. It must be concluded, given the test case, that the interview process is of marginal value in defining security needs.

The Second Method: Data Base Structure

One assumption that might be used is that a security system must be developed to protect the data elements from outside attack. Under this plan it is assumed that user needs will be satisfied should the data elements be protected adequately.

Data categories. The basic unit of information on a data base is the data element. A security plan must be designed to protect those data elements if the data base is to be an asset to the organization. Without protection of the data elements the data base becomes a liability.

To offer this protection, the data elements that will appear in the data base must be identified. In attempting to accomplish this task for the student data base, all possible data elements that are expected to be included were listed. This was done realizing that some elements might be deleted and others added before the data base is insti-

tuted. While this selection procedure might be considered a limitation, its effect will be minor given the extensive list that was generated and the fact that no user was able to suggest additional data elements.

The data elements that will be included in the data base fall into ten data categories. These are listed in Table 4-4. Note that each category is fairly self-explanatory and offers a fair prediction of the data elements that might appear in each.

Table 4-4

Data Categories

I Basic Classification and Identification Data

II Parent/Guardian and Permanent Name and Address Data

III Enrollment and Withdrawal Data

IV Local (on campus) Residence Information--Current

V Local (on campus) Residence Information--Future

VI Miscellaneous Billing Data

VII Academic Data

VIII Admissions Data

IX Miscellaneous Processing Data

X Fees

Under each category the data elements that were expected to be used were listed and assigned an identification number. When completed this listing of data elements should be identical to the data base's data element dictionary.

The listing that was prepared resulted from working closely with a staff member of Management Systems who was, at the same time, preparing the data element dictionary. From him, two primary sources provided most of the data element list. An MS publication of September 15, 1972, entitled Student Data Elements Dictionary contained a listing of all data items then used on tape and disk files. The National Center for Higher Education Management Systems at the Western Interstate Commission for Higher Education (WICHE) published Data Element Dictionary: Student in 1972. The WICHE report along with interviews with MS staff members, suplemented the list prepared from the MS publication.

As the WICHE report is a standard listing of all data elements in a typical student records system, and because it is employed by many universities, this second method can be generalized to any student records system in a university. Thus, not only the procedure employed here but the data elements listed as well, are easily generalized even though they were selected for this specific case.

In addition to data elements that are used extensively by the users, a number of elements fall into a category of processing items for each user department. These data elements might be required by the system for various processing functions or they could be elements that are created or updated automatically by the system based on some action taken by the user department. Fourteen categories were defined

for these data elements and are listed in Table 4-5. As these elements are maintained by the computer, they do not appear in the data element lists that follow.

Table 4-5

Processing Items

201	Admissions
202	Stats
203	Systems
204	Boston
205	Bursar
206	Registrar
207	Housing
208	Continuing Education
209	Financial Aid
210	Scheduling
211	Graduate School
212	Personnel
213	Stockbridge
999	Miscellaneous

Data element---creators. Once the data element list was prepared it was necessary to determine which users were the creators of which data elements. MS staff members aided in the preparation of this material which was later verified in user interviews. A complete list of data elements and the creators of those data elements appear in Appendix B.

An "X" appears under each user that has the power to create that particular data element. A number of elements have more than one entry. To understand this phenomenon

the admissions process must be explored.

When a student applies for admission to the University his records are processed through the Admissions Office. They establish a record for the student in an admissions file which contains admission information as well as much of the information in Data Categories I, II, and III. When that student is admitted his record is "rolled-over" to the "stats" file.

Based on this, the Admissions Office is the principal creator of most of the student data records. In some cases, students transfer in, re-enter the University, or for some other reason are not processed by the Admissions Office. In those instances, the Registrar creates the record in the "stats" file. It is estimated that less than 5% of all records are created in this manner.

The Graduate School is listed as the creator of some data elements. They act as both an Admissions Office and the Registrar for all graduate students. Because of this dual function, all graduate records on the "stats" file are initiated in the Graduate School.

Finally, some data elements don't have any creator listed. These elements are processing elements that are created by the system and not a user department. Some of these, such as "number of credits passed," are updated by the system at predictable intervals. Of the 123 data elements listed, 18 fall into this category.

Data element---accessors. Appendix C identifies those users who are allowed to access data elements in the data base. Access is defined as having permission to display that data element on a Cathode Ray Tube (CRT), print the data element out on a terminal, or to print it out in some batch reporting system.

Primary access is assumed which says that the operating system makes the decision to grant or deny access based on some predefined rules or schemes. The security system cannot be designed to control secondary access which is when information is passed from one user to another.

The appendix was prepared as a result of discussions with MS staff. Its contents were verified in user interviews. This access matrix represents the lowest level data usage.

Data element---updaters. Appendix D identifies the users that are allowed to update data elements on the data base. These users are allowed to make changes in each data element and, therefore, must also be allowed access to the data elements. Having authority to update records can be thought of as a second level of security which is below creation and above accessing of data elements.

Again, this appendix was prepared as the result of discussions with MS staff and then verified in user interviews. Each time that a "1" is entered it implies that that user has authority to update that data element.

Both the access matrix and update matrix can be used as authority matrices in the development of the security plan. Then when a request is made to access or update a data element the user's authority is verified in the appropriate matrix.

If authority is granted based on the information included in the matrix then it is of vital importance that the contents of the matrices are correct. There are two ways in which this can be accomplished. First, all data elements can be identified as data elements that the user should not have authority to access or update and will be labeled as such. It is assumed that all other data elements are within his authority structure.

A second method says that you start with the assumption that no one can access or update anything. From that starting point, you grant priviledges to users when you determine that they have a "need to know."

While the first method is the most popular it is also the least effective means of access control. Should an error occur when using the first mehtod, it is likely that access will be given to a user that shouldn't have access. In that case, it is also likely that this information will never become known because you have given him more than he needs to function but have not limited his information.

In the second case, an error is liable to mean that access has not been granted to someone who should have

access. Now information will be denied the user when he should have had access to it. It is a safe bet that the user will make this fact known while in the former situation that bet is not as safe.

The establishment of the data elements, their creators, updaters, and accessors is a worthwhile task for the reasons stated above. This information can then be used in authority matrices. However, little can be concluded about general security needs from this method of analysis.

It can be concluded that this is a necessary and sufficient procedure if we are to adequately protect all data elements from those who do not have authority to create, update, or access data elements. Conclusions relating to the consequences of various security breaches cannot be drawn from this method of analysis. Therefore, this method cannot be employed to totally define security needs but must be used in conjunction with other procedures for the establishment of a computer security package.

The Third Method: Data Element Usage

The underlying assumption in this part of the study is that users' security needs are a function of the frequency with which a particular data element is used. In other words, if a data element is used quite frequently by many user programs then destruction or modification of that data element could result in serious operational consequences to each of the users.

When a data base system is installed each data element is assigned a name that will be used by programmers when they write programs using the data base. In a non-data base environment common data names do not often exist.

To standardize data name usage in COBOL programs, MS established a COBOL data name directory. This directory lists each COBOL data name followed by the name of the program or programs that the COBOL data name appears in. It is expected that when a programmer writes a program that he will use the data names in this directory. Because COBOL has been the principal language used over the last several years, virtually all of the data elements maintained in files by the University appear in this directory.

As these data names will represent the starting point for the creation of the student data base it was felt that they could be used to analyze some of the information uses of the user departments. This analysis would be used in better understanding the security needs of the users.

Initially, MS provided a box of Hollerith cards which contained that subset of the COBOL data name directory which referenced student information. All of these names had identifying prefixes of "SU-" which were discarded. This information was then loaded onto a file for further processing.

Based on the data element numbers that had been previously assigned, each entry was given a number. A total

of 105 different data element names appear. This is somewhat lower than the 137 data elements that appear in Table 4-5 and Appendix B. Accounting for this discrepancy are two things. First, many data elements that are expected to be instituted in the new data base would not appear in the COBOL data name directory. Secondly, many of the existing programs were written in the older IBM programming language, AUTOCODER, so the data names would not appear in the COBOL directory.

Rank order usage. Appendix E is a listing of the frequency of occurrence of each data element in data element order. Thus, student number, which is data element #1, appears in 115 COBOL programs.

From this appendix, Appendix F was prepared which lists the frequency of occurrence of each data element in rank order of occurrence. Permanent address of the student's parent or guardian, which is data element #20, occurs in 209 programs.

Most frequently used. Because of the manner in which program names are assigned it is often easy to determine from the name what user department the program is used by. Eleven of the most frequently occurring departments were selected to be used in breaking down the manner in which the data elements were used.

Many of the department names are obvious from the past discussions but those that are not will be discussed. Ac-

counting handles the financial records of the University and works closely with the Bursar's Office. They require information about students for payments to trust funds, payments of dormitory bonds based on where the students reside, and many other bits of information.

Payroll requires access to student information for paying students who are working on campus. Note that the most frequently used items by them are the student's school address, the student name, and the student number.

Grades can be thought of as a subset of the Registrar's operation. An entire series of programs has been written which handle the grading process for the Registrar.

Entries under "Boston" indicate the usage of data elements in computer programs which have been written for special use by the University of Massachusetts-Boston campus. As ADP handles more of the computer work for Boston this list can be expected to grow.

The Registrar has two entries. The first entry applies to batch programs and the second entry applies to programs which are used on teleprocessing. This is the only department that can be broken down into these two categories.

As previously mentioned, "stats" is the primary data file for active student records. Many user departments have access to the "stats" file and there is no convenient way in which to isolate the accesses made by each department.

Finally, any reference that does not conveniently fall into any one of these categories was deposited in the miscellaneous group. Any number of user departments could have fallen into this area including Alumni Records, Personnel, and others.

Table 4-6 displays the 25 most frequently called for data names and identifies the number of times that each department uses the name. With 25 of 105 data names displayed we have only 23.8% of all data names but they account for 70.4% of all data name occurrences in the currently used COBOL programs.

It is this set of data that must be protected at a more secure level than the rest of the data base. Not only is it the most frequently used, but it is also the most interdependent. Therefore, when data element #20 is lost, each of the users suffers a loss. The situation is not quite as severe at the bottom of this list.

So, the three methods of analysis discussed, activity rank order is the most valuable. By offering protection to less than 24% of the data elements in this case we can protect over 70% of the data used by the programs currently running on the system.

No conclusions should be drawn about the relative importance of these data elements to a particular user department other than defining the number of times that a particular data element appears in programs written for that de-

Table 4-6

Most Frequently Called For Data Names and Departments Calling Them

Data Elements No.	Name	STATS	Registrar(Batch)	Registrar(TP)	Admissions	Housing	Scheduling	Boston	Financial Aid	Grades	Payroll	Accounting	Miscellaneous	Total
20	Permanent Address	108	1	13	6	15	13	17	5	2	2	8	19	209
79	Required Degree Subjects	95	17	55	0	11	3	0	0	16	0	0	0	197
202	Stats Processing	112	5	15	3	18	6	9	1	8	2	4	6	189
49	School Address (Current)	75	3	9	0	23	8	11	4	12	5	0	15	165
203	Systems Processing	84	2	9	1	16	9	9	1	3	2	0	5	141
4	Level	54	2	10	1	9	31	4	0	3	1	1	0	116
1	Student Number	70	3	2	2	8	6	9	0	3	4	2	6	115
3	Student Name	59	2	2	0	10	5	6	1	0	4	0	4	93
5	Class	54	3	6	1	5	6	7	0	3	1	2	3	91
32	Withdrawal Date	47	3	4	1	5	5	7	0	3	3	2	4	84
77	Credit/Point Data	46	2	8	1	3	2	8	2	4	0	0	2	78
99	Admissions Data	37	1	13	1	4	4	9	1	2	0	0	1	73
19	Parent/Guardian Address	42	4	6	0	0	4	0	0	0	0	0	4	60
15	Major Department	30	1	3	1	2	7	3	1	3	0	0	3	54
7	Sex	29	0	2	1	3	3	5	1	2	0	1	3	50
26	Entering Semester	26	1	4	1	4	4	3	1	2	0	0	2	48
10	Veteran	19	1	2	1	0	12	4	1	1	0	0	6	47
57	School Address Future	24	0	1	0	17	5	0	0	0	0	0	0	47
204	Boston Processing	19	0	4	0	1	4	8	1	1	1	0	2	41
116	Rent	15	0	1	0	1	4	7	1	2	2	0	4	37
8	Marital Status	30	0	2	1	2	10	2	3	0	1	0	2	36
78	Degree Credits	20	1	4	0	1	2	4	0	2	0	0	2	36
9	Date of Birth	18	0	3	1	5	2	3	1	0	0	0	2	35
100	Graduate Adm.Data	11	2	4	0	0	10	1	0	6	0	0	0	34
207	Housing Processing	6	0	4	0	21	1	0	0	0	0	0	1	33

partment. Clearly, some data element which is infrequently used might be critical to the department's operation.

By having cross tabulations on which departments use which data elements, policies can be established for recovery should a particular data element be destroyed or modified. For this reason alone, a clear understanding of the interdependence of these data elements is important. This third method of analysis adequately provides this information.

The Fourth Method: System Usage

Finally, we can make an assumption about how the computer system is utilized. This assumption says that a security plan must be developed which offers maximum protection when the system is most heavily used. Further, it might be possible to determine **when** users are using it **and** to give them added protection during their heavy usage periods.

It is fair to assume that the effect of a security breach will be greater when the system is heavily utilized. It is also fair to assume that users do not have identical periods in which they maximize their use of the system. This assumption has already been shown to be a fact. Based on this assumption, monthly accesses to the system were analyzed.

Monthly accesses. The University's operating system collects various teleprocessing statistics which might aid

in determining user security needs. Included is the number of accesses that each user made to the system each month. This identifies that a user accessed information but it does not tell us which data elements were accessed or which program was employed. In the event that a person makes a change to a data element, that event is not recorded in these statistics.

Table 4-7 lists the number of accesses per month in 1974 for each of eleven different users, total accesses that each user made in 1974, and the total accesses to the system for each of these months. Data for 1974 were selected because they represents the year in which teleprocessing was used most significantly by the University and, as such, it is believed that it is more representative of future computer utilization than previous years. Also, it is expected that users will satisfy more of their information needs with teleprocessing when the data base is instituted than with batch processing.

Two abnormalities are quite clear in looking at the raw data. First, Public Safety has virtually no entries for the first four months of the year. This is explained by the fact that they were having their teleprocessing terminals installed during that period which is a phenomenon that can be expected to occur each year as new users are put onto the system.

Table 4-7

Teleprocessing Accesses Per Month By User Departments For 1974

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
FINANCIAL AID	990	3518	703	2560	3977	13572	12116	11080	5819	6411	7291	10444	78481
GRADUATE SCHOOL	20068	20871	3974	13251	15754	19797	31242	22102	38869	15677	11966	12084	225655
HOUSING	4371	3338	687	1493	4576	7558	8212	19171	12210	3381	2020	8649	75666
REGISTRAR	59165	27909	13765	64903	78715	64591	91700	61950	59594	69791	89395	63348	744826
STOCKBRIDGE	3409	3377	1000	807	1898	5615	2928	1371	4765	3440	869	2440	31919
INSTITUTIONAL STUDIES	465	507	118	309	466	653	409	446	162	745	477	1106	5863
PROVOST	256	1443	291	388	1009	1560	508	1489	801	1180	1775	1828	12528
BURSAR	7455	8971	7752	16593	22174	22257	14571	16495	16100	13494	19685	21779	187326
TELEPHONE	12540	25712	3240	26699	23589	8329	5807	5474	63569	46602	41714	33118	296393
PUBLIC SAFETY	1	0	0	44	5920	6242	3018	3033	2531	4054	5139	5298	35280
A.D.P.	12020	2851	1050	6326	10396	7448	8280	8538	10634	7698	6366	7201	88810
TOTALS	120740	98497	32580	133373	168474	157622	178791	151149	215054	172473	186697	167295	1782747

Secondly, the data for March are exceedingly low. As no users perceive March as a peak usage month (see Table 4-3) this was initially thought to be the reason. After investigating it was found that virtual storage was being installed during March and that March was chosen for the installation as it was a non-peak period. During the installation the system was frequently down.

It must also be remembered that most of these statistics were gathered on the first shift. The second and third shifts are used to process batch jobs. Noting that, we find that an average of 6752 accesses are made per day given a 22 work day month and that during September, the peak month, that number reached 9775. Theoretically if the system is down for one day in September the amount of work that is backed up is one-half greater than on average. When the system is revived, it must not only complete a workload that is one-half greater than normal but must play catch up by being a day and a half behind as well.

In February, the least used month other than March, average daily accessing totals 4477 inquiries. This represents only 66% of an average day's operation. When the system is down for a day in February the situation is far less critical than in other periods. Recovery can occur quite easily as two days' work will not even be as great as one day's work during September.

Policy implications that can be drawn from this analysis are quite clear. Security needs are not constant over time. Certain periods of the year exist in which the demands on the system are twice as heavy as during other periods. It is during these periods that security should be the tightest. Recovery from a security breach can be more difficult during this period.

Looking at this exhibit along rows rather than columns we find another source of information. Users do not all use the system equally. The largest user, the Registrar, accesses the system 127 times more than the smallest user, Institutional Studies. The Registrar also accesses the system 2.5 times more than the second largest user, the Telephone Operators. In only one month, September, does the Registrar rank second in terms of computer usage.

While each user has his own unique problems, the Registrar is most dependent on the computer for his information needs. A shutdown of the computer could have a devastating effect on the operation of the Registrar's Office.

Percentage of monthly usage. From Table 4-7 it was possible to develop Table 4-8. This table shows the ratio of accesses made each month to the total number of accesses made by the user in the course of the year. If their access rate was constant then each block in the table would equal 8.33%.

This table allows us to get a feel for the actual peak periods rather than the perceived peak periods. It also

Table 4-8

User Departments Teleprocessing Accesses As A Percentage of Annual Use for 1974

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	TOTAL
FINANCIAL AID	1.26	4.48	0.90	3.26	5.07	17.29	15.44	14.12	7.41	8.17	9.29	13.31	4.40
GRADUATE SCHOOL	8.89	9.25	1.76	5.87	6.98	8.77	13.85	9.79	17.22	6.95	5,30	5.36	12.66
HOUSING	5.78	4.41	0.91	1.97	6.05	9.99	10.86	25.33	16.14	4.47	2.67	11.43	4.24
REGISTRAR	7.9	3.75	1.85	8.71	10.57	8.67	12.31	8.31	8.00	9.37	12,00	8.51	41.77
STOCKBRIDGE	10.68	10.58	3.13	2.53	5.95	17.59	9.17	4.30	14.93	10.78	2.72	7.64	1.79
INSTITUTIONAL STUDIES	7.93	8.65	2.01	5.27	7.95	11.14	6.98	7.61	2.76	12.71	8.14	18.86	0.33
PROVOST	2.04	11.51	2.32	3.10	8.05	12.45	4.05	11.89	6.39	9.42	14.17	14.59	0.77
BURSAR	3.98	4.78	4.14	8.86	11.84	11.88	7.78	8.81	8.59	7.20	10.51	11.63	10.51
TELEPHONE	4.23	8.67	1.09	9.01	7.96	2.81	1.96	1.85	21.45	15.72	14.07	11.17	16.63
PUBLIC SAFETY	0.00	0.00	0.00	0.12	16.78	17.69	8.55	8.60	7.17	11.49	14.57	15.02	1.98
A.D.P.	13.53	3.21	1.18	7.12	11.71	8.39	9.32	9.61	11.97	8.67	7.17	8.11	4.98

illustrates unusual changes in demand.

For instance, the telephone operators access the system most frequently in September. During September demand is nearly three times as great as average demand. Demand decreases slowly throughout the year from September on until very little usage of the system is made during June, July, and August. The usage pattern can be explained by noting that at the beginning of an academic year students do not know the telephone numbers of their friends but as the year goes on they learn their friends numbers and are less dependent on the telephone information service. Unlike other departments, should the system be down, access from the telephone operators will not back up. Students will obtain the information elsewhere rather than wait for the system to recover. Other usage patterns can be reviewed in much the same manner.

Percentage of annual usage. Table 4-9 was also developed from Table 4-7. Included in the body of the table is the percentage of the total month's usage that the user made each month. On the bottom of the table is the percentage of annual usage that all users made of the system that month.

This table, along with Table 4-8, provided the information to create Tables 4-10 and 4-11. Table 4-10 is a ranking of the number of accesses made each month while Table

Table 4-9

User Departments Teleprocessing Accesses As A Percentage of Total Monthly Use for 1974

	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC
FINANCIAL AID	0.82	3.57	2.16	1.92	2.36	8.61	6.78	7.33	2.71	3.72	3.91	6.24
GRADUATE SCHOOL	16.62	21.19	12.20	9.94	9.35	12.56	17.47	14.62	18.07	9.09	6.41	7.22
HOUSING	3.62	3.39	2.11	1.12	2.72	4.80	4.59	12.68	5.68	1.96	1.08	5.17
REGISTRAR	49.00	28.33	42.25	48.66	46.72	40.98	51.29	40.99	27.71	40.46	47.88	37.87
STOCKBRIDGE	2.82	3.43	3.07	0.61	1.13	3.56	1.64	0.91	2.22	1.99	0.47	1.46
INSTITUTIONAL STUDIES	0.39	0.51	0.36	0.23	0.28	0.41	0.23	0.30	0.08	0.43	0.26	0.66
PROVOST	0.21	1.47	0.89	0.29	0.60	0.99	0.28	0.99	0.37	0.68	0.95	1.09
BURSAR	6.17	9.11	23.79	12.44	13.16	14.12	8.15	10.91	7.49	7.82	10.54	13.02
TELEPHONE	10.39	26.10	9.94	20.02	14.00	5.28	3.25	3.62	29.56	27.02	22.34	19.80
PUBLIC SAFETY	0.00	0.00	0.00	0.03	3.51	3.96	1.69	2.01	1.18	2.35	2.75	3.17
A.D.P.	9.95	2.89	3.22	4.74	6.17	4.73	4.63	5.65	4.94	4.46	3.41	4.30
	6.77	5.52	1.83	7.48	9.45	8.84	10.03	8.48	12.06	9.67	10.48	9.38

Table 4-10

Monthly Accesses

Month	# of Accesses	% of Total
September	215,054	12.06
November	186,697	10.48
July	179,791	10.03
October	172,473	9.67
May	168,474	9.45
December	167,295	9.38
June	157,622	8.84
August	151,149	8.48
April	133,373	7.48
January	120,740	6.77
February	98,497	5.52
March	32,580	1.83

Table 4-11

User Accesses

User Department	# of Accesses	% of Total
Registrar	744,826	41.77
Telephone	296,393	16.63
Graduate School	225,655	12.66
Bursar	187,326	10.51
A.D.P.	88,810	4.98
Financial Aid	78,481	4.40
Housing	75,666	4.25
Public Safety	35,280	1.98
Stockbridge	31,919	1.79
Provost	12,528	0.77
Institutional Studies	5,863	0.33

4-11 is a rank order listing of the amount of usage that each user made during the year.

Peak usage periods. Table 4-10 differs sharply from the perceived peak usage patterns exhibited in Table 4-3. In both cases September was determined to be the peak usage period and March to be one of the least used months but any similarities stop at that point.

The users selected January as the second most important month but the teleprocessing statistics show it to be the tenth. Similarly, November was not selected by any to be a peak usage period but the teleprocessing statistics show it to be the second most important month. Similar inconsistencies apply to other months.

Inconsistencies such as the above imply two things. First, users may not be able to accurately estimate the peak computer usage periods due to any number of factors of their definition of peak period could be different than that of the researcher. Secondly, an attempt to measure security needs on the basis of usage might be difficult unless the inconsistencies in perceived peak periods can be explained.

There is also the difficulty of comparing apples and oranges. In this case, we are comparing teleprocessing statistics, which represents actual usage, against their perceptions of peak usage periods employing the assumption that as the work-load rises or falls in the user's office his use of teleprocessing will rise and fall by a similar amount.

Based on user interviews and these teleprocessing statistics this assumption is false.

User classifications. The other table lists the annual usage of each user and his percentage of annual use. Clearly, the Registrar uses the system more than any other user and uses nearly 42% of the total system's resources and over half of the accesses in July are made by the Registrar.

This table suggests a possible division of users into five classes which are presented in Table 4-12. Recovery from a security breach could then be based on user class. All efforts would be made to resume services to Class A members with efforts filtering down as services are re-instituted for a user class.

A variation of this theme might be to establish class membership for each individual month. This would consider the user's peak usage period in determining membership class.

Another variation might lump together classes to produce larger classes with bounds which are less precisely defined. This could create classes with large memberships which might then require that recovery resources would have to be spread too thin among class members.

The assumption behind this approach is that the amount of computer usage is the key determinant of security needs. In some installations that assumption might be true but it cannot be taken on blind faith.

Table 4-12

Suggested User Classes

Class	Bounds	Members
A	25% to 100%	Registrar
B	10% to 24.99%	Telephone Graduate School Bursar
C	2% to 9.99%	A.D.P. Financial Aid Housing
D	1% to 1.99%	Public Safety Stockbridge
E	0% to 0.99%	Provost Institutional Studies

For example, comparing the Telephone Operation with the Graduate School would lead us to believe that loss of the computer would be more difficult for the Telephone Operation to bear than the Graduate School. The Telephone Operation is an inquiry operation only that can be without the system with few or no consequences. It is true that students would be unable to obtain telephone numbers that they want but that would cut back a service which has little economic impact on the University.

The Graduate School uses the computer to update records as well as to make inquiries. When the system is down the updating becomes backed up which creates a work overload for its office staff. This situation is quite different from the Telephone Operation as records are not updated.

A fair compromise would be to evaluate the operational effect of a security breach on each class member. If the effect is greater than the average class member's, the user could be pushed up to the next higher class. Similarly, if the effect is less than the average class member's, the user could be pushed down to the next lower class. This should be done for each month to account for peak usage and the operational effect that month.

It can be concluded from the system usage analysis that peak usage periods are easily discernible and that user departments which heavily utilize the computer system can be easily identified. One must be careful not to make deductions from this data by reviewing it in isolation. Heavy system usage does not perfectly equate with a need for strong security because at least one user, the Telephone Operation, could go without the system and not be adversely affected.

System usage analysis for peak periods was found to conflict with the perceived peak usage periods as identified by user departments. Because of this inconsistency, one cannot draw any specific conclusions about peak periods until the reason for this inconsistency is discovered.

It can be concluded that information obtained from this analysis is necessary but not sufficient for determining security needs. This method of analyzing security needs must be supplemented by other methods.

The Four Methods Reviewed

Security needs are different in a data base environment than in the traditional setting. This situation results from the condition that an action by one user could adversely affect a great number of users or all users.

Four alternatives for estimating security needs have been suggested. These alternatives were reviewed in a university setting to determine their validity in measuring security needs. It was found that none of these alternatives shed much light on user security requirements in this particular situation.

Collecting various pieces of data to define security needs is not a complete answer to this problem. It is, however, effective in the establishment of authority matrices and for an understanding of system usage patterns.

From the user interviews one might conclude that security is an unimportant issue. With respect to student records and minor problems that can occur, this may be true. Surely the on-line system at the University is not as critical as a similar system in operation at BankAmericard. Gross problems are the ones that users are unwilling to consider the possibility of occurring. These are the events that have not as yet occurred but, if they ever do, will cause great operational problems to the University.

A fifth method proposed. Another method that might be suggested would be to keep a log of the occurrence of security breaches. This log could then be used to estimate the probability of an event or a class of events occurring. In fact, a number of security breaches have already occurred on the University of Massachusetts campus with only a couple of them directly related to student records. Because they are indicative of possible future security breaches in student records some examples are presented below:

1. During the Spring of 1975 master keys were found to be missing for over 2100 offices on campus. The missing keys allow access to the University Research Computing Center as well as most of the research laboratories on campus.
2. A fire in Tobin Hall destroyed scientific experiments that had been in progress for many years. In addition to losing irreplaceable research data, a minicomputer, valued at over $10,000, was destroyed.
3. Many years ago, a female student employee in the Registrar's Office was discovered altering records of another student. The employee had been dating the other student, a football player. She was attempting to alter his records to maintain his football eligibility.
4. During the Spring of 1975, many mischievous students were able to determine sign-on codes for students using the University Research Computing Center by finding these numbers on discarded printouts. Because each

user was able to assign his own passwords, but seldom did, and because sign-on codes ran sequentially for a block of numbers, these students were able to sign-on and randomly create passwords for that number and other numbers that followed in sequence. When the owner of the number next attempted to sign-on, he was denied access by the system because he did not know the password.

5. In the Fall of 1974, the scheduling run was stopped as a result of a machine error. When it was restarted, inadequate restart procedures resulted in a large proportion of students being given empty schedules. Owing to the lateness resulting from the re-run, a decision was made to issue the schedules which later resulted in havoc at the Scheduling Office.

6. In two unrelated cases terminals were installed in user departments with incorrect accessing capabilities. In one case, the user was not given sufficient accessing authority which resulted in ADP being immediately informed and the situation corrected.

The reverse occurred in the other case. The user was granted excessive accessing powers that were not uncovered until a representative of the Provost's Office was passing through the user's office and noticed employees accessing information beyond their "need to know." His discovery led to a quick reversal

of the situation.

7. During the Fall of 1973, a new parking system was being installed on campus. The new system called for greatly increased parking fees which were being opposed by the University employees' union and the student body.

Management Systems was responsible for programming the billing system as well as the space allocation system. A full-time programmer who was assigned to the project went on an extended vacation owing to suspected union pressure. To complete the project, a graduate student was employed.

Near the completion date of the project, the graduate student stopped coming to work and was fired. It was then discovered that the nearly completed system was "booby trapped" to prevent it from working properly. Only a crash programming effort prevented the parking system from being completely sabotaged.

8. On numerous occasions the administration building has been taken over by student groups. In no case have computer operations been interrupted by these disruptions except for preventing key personnel from entering the building.

Because these events have <u>already</u> occurred, security cannot be ignored. Many of the users' less obvious security

needs could be satisfied if many of the gross problems that can cause catastrophes could be prevented.

By maintaining a log of the events which have created security problems on campus, we may come closer to defining users' security needs than any of the other four methods suggested by determining gross problems and developing countermeasures for them. It is clear from this study that user departments are not willing to consider security problems. Perhaps this fifth method will demonstrate to those users that security is, in fact, an important issue worthy of consideration.

Factors of a university security plan. Although the study failed to expose clear procedures for defining security needs, six important factors of an adequate data base security plan in a university setting have become apparent. These are:

1. User departments must be aware of possible security breaches, the effect of those breaches on their departments, and their roles in preventing the breaches from occurring.
2. A clear definition must exist of the control of data elements within the data base.
3. Adequate physical security measures must be established to prevent illegal access to the computer center and to prevent destruction from Acts of God.

4. Usage of key data elements must be monitored to prevent accidental or intentional destruction, modification, or disclosure.
5. Adequate restart and recovery procedures must be established to prevent the modification of the data base in the event of machine failure.
6. Key data elements, up-to-date programs, and documentation for those programs must be backed up in an offsite location.

These factors can be thought of as minimum considerations. However, their implementation will eliminate many of the gross security breaches that might occur in a typical university setting and will, therefore, satisfy many of the users' needs.

In the next chapter we will review what has been suggested by this study and review its basic limitations. Finally, we shall make recommendations for future study.

C H A P T E R V

CONCLUSIONS

It was the purpose of this study to review various methods for defining security needs in a data base environment. The selection of this topic was based on the assumption that security needs vary based on the user's application of the computer system. However, little is known about these needs so that security plans are developed without much consideration given to the value of the plan versus the value of what it should be protecting. If needs can be defined then a security plan can be developed which minimizes costs and maximizes protection.

Security is a complex issue. Users are not able to say that conditions in their departments require that locks be put on the computer room doors, or that files be backed up, or that access restrictions be imposed. Staff in Management Systems and Administrative Data Processing are unable to do this as well. It is difficult to define need in relation to various countermeasures.

Defining needs in relation to various threats is more easily accomplished. For example, it is much easier to determine the outcome on a user department of a fire that puts the computer out of business than to determine the value of the fire detection equipment to each department.

It was thought, then, that security needs would be best

estimated when viewed from the effect that they would have on the user departments. It was also believed that this would be the easiest to estimate by the various user departments.

Summary

At the beginning of the study it was noted that the intention of this paper was to be an exploratory field study in a university setting. The first chapter presented a quick overview of the problem with defining security needs and described how we were going to pursue it.

In the second chapter a general discussion was presented of various work that has been done in computer security. This material was presented to give the reader an introduction to the subject of computer security and explain a number of terms that are unique to the field. While the material is not complete, it does present an overview of the relevant material that has been written about the subject matter. Each important part of a security plan was presented and described in some detail.

The premise underlying the third chapter is that security needs are the foundation of any security plan. This chapter contained several sections: (1) Without a clear understanding of needs, an adequate security plan is impossible to construct. Likewise, it is important that the structure of security plans be clearly understood if this

foundation is to be the proper one. So, because we considered security needs in a data base environment, the structure of data bases must be understood. Thus, we discussed data organization, key data characteristics, and the problems of data base design. (2) Further, the third chapter described how data is stored in a problem solving environment rather than in a user oriented environment. Data elements are stored once which, although saving storage space and updating time, creates an interdependence among users not traditionally found. Increased management flexibility is gained at the loss of data independence. (3) And, in addition, design criteria for a security plan were presented. It was pointed out that the relationships between these variables have not been adequately explored. (4) Finally, it was suggested that as more funds are committed to a security plan, the probability of detection will increase. While no hard evidence supports this conclusion, it was made on the assumption that an intruder would be less likely to attempt to breach the system should he feel that his probability of being uncovered is increased. As he notices more efforts going into the security plan then he perceives that his chances of getting caught will increase. The inverse of this relationship was also suggested.

All of these variables and their entwining relationships make up a functional security plan. However, these

relationships are not understood today.

In the fourth chapter, four initial and alternative methods of determining security needs in a university setting were suggested. That setting, as well as a control problem in that setting, were discussed.

It was recommended that the data base administrator be the controller of the entire data base and would act as an agent of the Users' Advisory Committee. This is considered to be a necessary security requirement to maintain the integrity of the data base by preventing a proliferation of various security procedures from all of the user departments.

1. As the first method of defining security needs, it was suggested that users be interviewed. These interviews proved less than satisfactory in providing a definitive list of security needs, but they did provide valuable insights into the operation of the user departments.

Users, in general, were unable to estimate the effect of losing, modifying, or disclosing individual records or the entire data file. However, they were able to provide estimates of the effect on their departments should the computer be "down" for any length of time, but even then their estimates of peak usage periods were inconsistent with other findings to be presented later. It is apparent that they have not given ample consideration to security problems.

Written operational procedures for the use of the computer system and the distribution of computer resident in-

formation in most users' departments is non-existent. Disaster plans, as well, are non-existent.

User support is required to insure that security risks are minimized and that recovery, should it be necessary, is rapid. Based on the interviews conducted, this support and interest were not found to exist.

2. A second method proposed was to define a complete list of data elements and to identify those users that have the ability to create, update, and/or access these data elements. It was found that this procedure offers information about how the data base will be constructed and how it will be used. It also provides for the establishment of authority matrices which is this method's greatest value. In addition, it might be possible to determine how to physically construct the data base dependent on a commonalty of uses of data elements.

3. Segmenting data elements according to frequency of use was a third method. From this method we were able to determine which data elements are most frequently used. It was also possible to determine which data elements were used by many of the user departments.

This method identified the data elements which must be more frequently backed up and monitored for illegal access attempts. As the data base will be quite large, all data elements will not be backed up or monitored and a procedure for establishing a priority is necessary.

4. The fourth method reviewed was that of system usage. By reviewing the manner in which the system is utilized we were able to identify actual peak usage periods. The utilization pattern that evolved could be used as an aid in developing an adequate security plan.

It is important that utilization information not be used in a vacuum. Other information, such as that obtained in user interviews, will verify or refute the conclusions drawn from utilization studies. In fact, inconsistencies between the user interviews and the utilization studies were found to be significant. From this study it is clear that a security plan must be developed around the Registrar's system usage.

A fifth method was suggested after it was concluded that the other four methods were of marginal value in defining security needs. It was suggested that a log be maintained of security breaches to generate occurrence probabilities for these events and to dramatize to the user departments that security breaches can occur.

A general conclusion that might be drawn from this project is that the four original methods suggested might have little value in defining security needs in <u>any</u> university setting. As the data elements were developed from the WICHE report and are, therefore, standard in many universities, it is fair to assume that the conclusions suggested here could apply to other universities as well.

A glimmer of hope exists in the fifth method proposed. It might be possible to log security breaches for a large number of universities. Statistical analysis of these cases could then be used to determine university security needs based on statistics gathered from actual cases.

Limitations of The Study

The very nature of an exploratory study makes it quite limited. It was the purpose of this study to look at security needs in a university data base environment and to review alternatives about defining those needs. Conclusions based on statistical tests are impossible and impractical until more is learned about how to determine these needs. Therefore, results are based on insights suggested rather than conclusions that have been proven.

As the test site was a university, it might be dangerous to generalize to a commercial environment. Nevertheless, many of the insights uncovered here might be applicable to those settings.

Security is highly individualized. Each computer installation has a different set of needs that must be determined to develop its own security plan. While a limitation might be that little of what we have learned is transferable, that is a limitation of security plans rather than of this particular study.

The logging of security breaches in only one case provides little information to generalize from. If logs of security breaches could be compiled for a large number of academic institutions, then the results could be used to establish occurrence probabilities. From these logs we might have been able to establish the two or three most serious security problems.

Finally, security issues are by their very nature private which results in people being unwilling to openly discuss their problems. Therefore, a complete set of security breaches which directly relate to individual security needs is never possible to obtain. This is compounded by the fact that security is dynamic which simply means that new ways to covertly obtain information from a computer system are always being discovered.

In spite of these limitations, this exploratory study has uncovered some valuable insights into the security needs problem. Some of these insights include that users can be classified according to use of the system or their expected harm should the system be down, the data base can be segmented by its most vulnerable data elements, and users' perceptions of peak usage periods are not always accurate. Defining security needs will never be an exact science but, perhaps, some inroads have been made in looking at the important issues.

Areas for Further Research

It is not difficult to define areas of computer security that are open to further research. Computer security is a new area of concern that remains more of an art than a science. The range of research topics will continue to grow as new computer systems are developed and new computer uses defined. However, the areas mentioned here will only relate to those topics uncovered while working on this study.

First, the relationships between effectiveness, economy, simplicity, and reliability must be further explored. As these relationships become clearer, we will move one step closer to being able to develop cost effective plans.

Second, establishing procedures for defining objective functions of security plans will also extend a user's ability to create his own cost effective plan. Various objective functions might be suggested and security plans developed to meet those objective functions. It might then be possible to generalize objective functions to various computer environments.

Third, would be a review of the functioning of a computer system to determine if the system utilization pattern suggests a security plan that dynamically changes based on the changing system usage patterns. Research such as this might be very difficult to accomplish but its value to the protection of computer systems could be beneficial.

Fourth, much research is still required to define individual security needs. The variables that enter into this determination are not clearly defined. They must be identified for differing user environments.

Finally, of the material published about security, much of it is too general for direct application to unique situations. In cases where individuals have taken a unique approach to solving their security problems, they have been unwilling to publish the procedures that they went through. While this is quite understandable, more has to be published so that all computer users might benefit from their experiences. The future of computer security research lies in the willingness of all to share their knowledge and experiences.

SELECTED BIBLIOGRAPHY

"A Computer Security Survey," Modern Data, Vol. 7, No. 7 (July, 1974), 52.

AFIPS Systems Review Manual on Security. Montvale, N.J.: AFIPS Press, 1974.

Alexander, Tom. "Waiting for the Great Computer Rip-off," Fortune, Vol. 90, No. 1 (July, 1974), 143-150.

Allen, Brandt. "Danger Ahead! Safeguard Your Computer," Harvard Business Review, Vol. 46, No. 6 (November-December, 1968), 97-101.

Babcock, J.D. "A Brief Description of Privacy Measures in the RUSH Time-Sharing System," Spring Joint Computer Conference, Vol. 30 (Spring, 1967), 301-302.

Bates, William S. "Security of Computer-Based Information Systems," Datamation, Vol. 16, No. 5 (May, 1970), 60-65.

Bensoussan, A.; Clingen, C.T.; and Daley, R.C. "The Multics Virtual Memory: Concepts and Design," Communications of the ACM, Vol. 15, No. 5 (May, 1972), 308-318.

Berg, John L. "Data Security and Privacy: There Is A Difference," Modern Data, Vol. 7, No. 9 (September, 1974), 52.

Bergart, Jeffrey G.; Denicoff, Marvin; and Hsiao, David K. An Annotated and Cross-Referenced Bibliography on Computer Security and Access Control in Computer Systems. The Computer and Information Science Research Center, The Ohio State University, Columbus, Ohio, November, 1972.

Borgerson, Barry R. "Dynamic Configuration of System Integrity," Fall Joint Computer Conference, Vol. 41, Part I (Fall, 1972), 89-96.

Boruch, Robert F. "Relations Among Statistical Methods for Assuring Confidentiality of Social Research Data," Social Science Research, Vol. 1, No. 4 (December, 1972), 403-414.

_____. "Security of Information Processing - Implications from Social Research," Fall Joint Computer Conference, Vol. 41, Part I (Fall, 1972), 425-433.

Boruch, Robert F. "Strategies for Eliciting and Merging Confidential Social Research Data," Policy Science, Vol. 3 (1972), 275-300.

Boruch, Robert F. and Endruweit, Gunter. "Mathematical Methods to Assure Confidentiality and Anonymity of Research Data," Zeitschrift fur Soziologic, Vol. 2, No. 3 (July, 1973), 227-238.

Browne, Peter S. "Computer Security-A Survey," Database, Vol. 4, No. 3 (Fall, 1972), 1-12.

Canning, Richard G. "Computer Fraud and Embezzlement," EDP Analyzer, Vol. 11, No. 9 (September, 1973), 1-14.

_____. "Computer Security: Backup and Recovery Methods," EDP Analyzer, Vol. 10, No. 1 (January, 1972), 1-15.

_____. "Data Security in the CDB," EDP Analyzer, Vol. 8, No. 5 (May, 1970), 1-14.

_____. "Protecting Valuable Data--Part 1," EDP Analyzer, Vol. 11, No. 12 (December, 1973), 1-13.

_____. "Protecting Valuable Data--Part 2," EDP Analyzer, Vol. 12, No. 1 (January, 1974), 1-14.

_____. "Security of the Computer Center," EDP Analyzer, Vol. 9, No. 12 (December, 1971), 1-13.

Carrol, John M.; Martin, Robert; McHardy, Lorine; and Moravec, Hans. "Multi-Dimensional Security Program for a Generalized Information Retrieval System," Fall Joint Computer Conference, Vol. 39 (Fall, 1971), 571-577.

Chu, Albert L.C. "The Corporate Achilles Heel," Business Automation, February, 1971, 33-38.

CODASYL Data Base Task Group Report, New York: Association for Computing Machinery, April, 1971.

CODASYL Systems Committee. Feature Analysis of Generalized Data Base Management Systems, New York: Association for Computing Machinery, May, 1971.

Comber, Edward V. "Management of Confidential Information," Fall Joint Computer Conference, Vol. 35 (Fall, 1969), 143.

Computer Control Guidelines. Toronto: The Canadian Institute of Chartered Accountants, 1970.

"Computer Security," E & E, Vol. 13, No. 2 (Summer, 1975), 2-9.

Conway, R.W.; Maxwell, W.I.; and Morgan, H.L. "On the Implementation of Security Measures in Information Systems," Communications of the ACM, Vol. 15, No. 4 (April, 1972), 211-220.

Copeland, Peter. Private interview at Milton Bradley, East Longmeadow, Ma., April 24, 1974.

Corbato, F.J.; Saltzer, J.H.; and Clingen, C.T. "Multics - The First Seven Years," Spring Joint Computer Conference, Vol. 40 (Spring, 1972), 571-581.

Courtney, Robert H. "A Systematic Approach to Data Security," U.S. National Bureau of Standards Symposium on Privacy and Security in Computer Systems, Washington, D.C., March, 1974.

_____. Private interview at IBM, Poughkeepsie, N.Y., July 22, 1974.

Davis, Gordon. Auditing and EDP, New York: American Institute of Certified Public Accountants, 1968.

Denning, Peter J. "Third Generation Computer Systems," Computing Surveys, Vol. 3, No. 4 (December, 1971), 175-216.

Dijkstra, Edsger W. "The Structure of 'THE'-Multiprogramming System," Communications of the ACM, Vol. 11, No. 5 (May, 1968), 341-346.

Dirks, Raymond L. and Gross, Leonard. The Great Wall Street Scandal, New York: McGraw-Hill, 1974.

Evans, Arthur, Jr.; Kantrowitz, William; and Weiss, Edwin. "A User Authentication Scheme Not Requiring Secrecy in the Computer," Communications of the ACM, Vol. 17, No. 8 (August, 1974), 437-441.

"Ford Signs Privacy Bill," Computerworld, Vol. 9, No. 2 (January 8, 1975), 1.

Friedman, Theodore D. and Hoffman, Lance. "Execution Time Requirements for Encipherment Programs," Communications of the ACM, Vol. 17, No. 8 (August, 1974), 445-449.

Glaser, Edward L. "A Brief Description of Privacy Measures in the Multics Operating System," Spring Joint Computer Conference, Vol. 30 (Spring, 1967), 303-304.

Graham, G. Scott and Denning, Peter J. "Protection-Principles and Practice," Spring Joint Computer Conference, Vol. 40 (Spring, 1972), 417-429.

Hansen, Morris H. "Insuring Confidentiality of Individual Records in Data Storage and Retrieval for Statistical Purposes," Fall Joint Computer Conference, Vol. 39 (Fall, 1971), 579-585.

Hemphill, Charles F., Jr. Security for Business and Industry, Homewood, Ill.: Dow Jones-Irwin, Inc., 1971.

Hewitt, Donald O. "Computer Security in an Educational Environment," unpublished Masters thesis, Massachusetts Institute of Technology, 1973.

Hoffman, Lance J. "Computers and Privacy: A Survey," Computing Surveys, Vol. 1, No. 2 (June, 1969), 85-103.

_____, ed. Security and Privacy in Computer Systems, Los Angeles: Melville, 1973.

_____. "Security Ratings for Computer Systems," Electronics Research Laboratory, College of Engineering, University of California, Berkeley (Memorandum No. ERL-M-444), May 20, 1974.

_____. "The Formulary Model for Flexible Privacy and Access Control," Fall Joint Computer Conference, Vol. 39 (Fall, 1971), 587-601.

Hsiao, D.K.; Kerr, D.S.; and McCauley III, E.J. A Model for Data Secure Systems (Part I), The Computer and Information Science Research Center, The Ohio State University, Columbus, Ohio, February, 1974.

Hsiao, D.K.; Kerr, D.A.; and Nee, C.J. Context Protection and Consistent Control in Data Base Systems (Part I), The Computer and Information Science Research Center, The Ohio State University, Columbus, Ohio, February, 1974.

Kahn, David. The Code Breakers, New York: Macmillan, 1967.

Katzan, Harry, Jr. Computer Data Security, New York: Van Nostrand Reinhold Company, 1973.

Krauss, Leonard I. SAFE: Security Audit and Field Evaluation for Computer Facilities and Information Systems, East Brunswick, N.J.: Firebrand, Krauss and Company, Inc., 1972.

Kuong, Javier F. Computer Security, Auditing and Controls: A Bibliography, Wellesley Hills, Ma.: Management Advisory Publications, 1973.

_____. Computer Security, Auditing and Controls: Text and Readings, Wellesley Hills, Ma.: Management Advisory Publications, 1974.

_____. Private interview at Management Advisory Publications, Wellesley Hills, Ma., July 12, 1974.

Lampson, B.W. "Dynamic Protection Structures," Fall Joint Computer Conference, Vol. 35 (Fall, 1969), 27-38.

Leavitt, Don. "IBM Project Chief Finds 90% of Sites Lack Orderly Security Plan," Computerworld, Vol. 8, No. 19 (May 8, 1974), 1.

Leibholz, Stephen W. and Wilson, Louis D. Users' Guide to Computer Crime, Randor, Pa.: Chilton Book Company, 1974.

Linde, R.R.; Weissman, S.; and Fox, C.E. "The ADEPT-50 Time-Sharing System," Fall Joint Computer Conference, Vol. 35 (Fall, 1969), 39-50.

Lipner, Steven B. "Computer Security Research and Developments," The Mitre Corporation, Bedford, February, 1973.

Madnick, Stewart. Private interview at Sloan School of Management, Massachusetts Institute of Technology, Cambridge, Ma., January 22, 1974.

Martin, James. Security, Accuracy, and Privacy in Computer Systems, Englewood Cliffs, N.J.: Prentice-Hall, 1973.

Martin, James and Norman, Adrian R.D. The Computerized Society, Englewood Cliffs, N.J.: Prentice-Hall, 1970.

Martin, James S. Data Element Dictionary: Student, 2nd ed. Boulder, Colorado: National Center for Higher Education Management Systems at Western Interstate Commission for Higher Education, 1972.

Miller, Arthur R. The Assault on Privacy: Computers, Data Banks, and Dossiers, Ann Arbor, Mich.: The University of Michigan Press, 1971.

Miller, Arthur. "The Dossier Society-Cybernetics and Surveilance," MBA, Vol. 5, No. 3 (March, 1971), 30-32.

Nolan, Richard L. "Computer Data Bases: The Future is Now," Harvard Business Review, Vol. 51, No. 5 (September-October, 1973), 98-114.

Owens, Richard C., Jr. Primary Access Control in Large-Scale Time-Shared Decision Systems, Cambridge, Ma.: Project MAC, Massachusetts Institute of Technology, July, 1971.

Parker, Donn B. Manual for Investigation of Computer-Related Incidents of Intentionally Caused Losses, Injuries, and Damage, Livermore, California: Lawrence Livermore Laboratory, University of California, February, 1973.

_____. Threats to Computer Abuse, Livermore, Calif.: Lawrence Livermore Laboratory, University of California, March, 1973.

Parker, Donn B.; Nycum, Susan; and Oura, S. Stephen. Computer Abuse, Menlo Park, California: Stanford Research Institute, November, 1973.

Peters, Bernard. "Security Considerations in a Multi-Programmed Computer System," Spring Joint Computer Conference, Vol. 30 (Spring, 1967), 282-286.

Petersen, H.E. and Turn, R. "System Implications of Information Privacy," Spring Joint Computer Conference, Vol. 30 (Spring, 1967), 291-300.

Podgus, Christopher. "Outwitting the Computer Swindler," Computer Decisions, Vol. 5, No. 9 (September, 1973), 12-16.

Porter, W. Thomas, Jr. "Computer Raped by Telephone," The New York Times Magazine, September 8, 1974, 32-43.

_____. EDP Controls and Auditing, Belmont, California: Wadsworth Publishing Company, 1974.

"Privacy in Information Systems," Secure Automated Facility Environment Project, The State of Illinois, 1974.

Purdy, George B. "A High Security Log-in Procedure," Communications of the ACM, Vol. 17, No. 8 (August, 1974), 442-444.

Records, Computers, and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems, U.S. Department of Health, Education, and Welfare, Washington, D.C., July, 1973.

"Requirements for a Data Base Management System," The Joint GUIDE and Share Data Base Requirements Group, New York Share, Inc., November 11, 1970.

Saltzer, Jerome H. "Protection and the Control of Information Sharing in Multics," Communications of the ACM, Vol. 17, No. 7 (July, 1974), 388-402.

Scherf, John Arthur. Computer and Data Security: A Comprehensive Annotated Bibliography, Cambridge, Ma.: Massachusetts Institute of Technology, Sloan School of Management, 1974.

Sharpe, William F. The Economics of Computers, New York: Columbia University Press, 1969.

Skatrud, R.O. "A Consideration of the Application of Cryptographic Techniques to Data Processing," Fall Joint Computer Conference, Vol. 35 (Fall, 1969), 111-117.

Sorensen, J.L. "Common Sense in Computer Security," Journal of Systems Management, Vol. 23, No. 4, 12-14.

"Standards for Internal Bank Auditing in an Electronic Data Processing Environment. Bank Administration Institute, Park Ridge, Ill., 1972.

Student Data Elements Dictionary. Amherst, Ma.: University of Massachusetts, September 15, 1972.

Turn, Rein. "A Brief History of Computer Privacy/Security Research at Rand," The Rand Corporation, P-4798, March, 1972.

____. "Privacy and Security in Personal Information Databank Systems," The Rand Corporation, R-1044-NSF, March, 1974.

____. "Privacy Transformations for Databank Systems," National Computer Conference, 1973, 589-601.

____. "Toward Data Security Engineering," Rand Corporation, P-5142, January, 1974.

Turn, R.; Fredrickson, R.; and Hollingworth, D. "Data Security Research at the Rand Corporation: Description and Commentary," The Rand Corporation, P-4914, October, 1972.

Turn, Rein and Shapiro, Norman A. "Privacy and Security in Databank Systems--Measures of Effectiveness, Costs, and Protector-Intruder Interactions," Fall Joint Computer Conference, Vol. 41, Part I, (Fall, 1972), 435-444.

Van Tassel, Dennis. Computer Security Management, Englewood Cliffs, N.J.: Prentice-Hall, 1972.

Ware, W.H. "Computers in Society's Future," The Rand Corporation, P-4684, August, 1971.

____. "Records, Computers and the Rights of Citizens," Datamation, Vol. 19, No. 9 (September, 1973), 112-114.

____. "Security and Privacy in Computer Systems," Spring Joint Computer Conference, Vol. 30 (Spring, 1967), 279-282.

____. "Security and Privacy: Similarities and Differences," Spring Joint Computer Conference, Vol. 30, (Spring, 1967), 287-290.

Wasserman, Joseph J. "Plugging the Leaks in Computer Security," Harvard Business Review, Vol. 47, No. 5 (September-October, 1969), 119-129.

Weissman, C. "Security Controls in the ADEPT-50 Time-Sharing System," Fall Joint Computer Conference, Vol. 35 (Fall, 1969), 119-133.

Westin, Alan F. Privacy and Freedom, New York: Atheneum, 1967.

Westin, Alan F. and Baker, Michael A. Databanks in a Free Society: Computers, Record-Keeping and Privacy, New York: Quadrangle, 1972.

Woodward, Franklin G. and Hoffman, Lance J. "Worst-Case Costs for Dynamic Data Element Security Decisions," Electronics Research Laboratory, College of Engineering, University of California, Berkeley (Working Paper), 1974.

Woolridge, Susan; Corder, Colin R.; and Johnson, Claude R. Security Standards for Data Processing, London: Macmillan, 1973.

APPENDIX A

APPENDIX A

Registrar

Interviewees - Ralph Jones
Douglas Sutherland
Marion Markwell

Function - Acts as the central record-keeping agency of the university for student records.

Information Needs -

Have extensive power to update and access student records. Can create new records for students which were not created in the admissions office. Also, creates grade records. Has the most extensive information needs of any user of the data base

Graduate Registrar

Interviewee - Robert Swasey

Functions - Acts both as an admissions officer and registrar for the graduate school. Responsible for all graduate records from application for admission until graduation or other termination.

Information Needs -

Information needs parallel those of the undergraduate admissions office and the undergraduate registrar. Have the power to create, update, and access all graduate records.

Bursar

Interviewee - Robert Mishol

Function - Bills both undergraduate and graduate students for services of the university. Collects and records payments.

Information Needs -

Requires access to all student records relevant to the billing function. Can create and update elements related to bill payment. Information needs increase at various times of the year.

Admissions

Interviewee - Robert Doolan

Function - Reviews applications for admissions and readmission to the university and acts accordingly.

Information Needs -

Student "stats" records are created by Admissions from the application and Princeton scores which becomes the principal data base record when the student is accepted at the university. While they are the principal creator of the data record they have no power to create or update items on the "stats" record once it is turned over to the registrar.

Housing

Interviewee - J. Bruce Cochrane

Function - Assign students to dormitories on campus. Make changes to student's current address. Control funding for bond payments.

Information Needs -

Access address information and other relevant information such as birth-date, marital status, and veteran status. Can up-date address information and creates new address data elements. Will have increased information needs in conjunction with the increased responsibilities of the Office of Residental Life.

Financial Aid

Interviewee - Richard Dent

Function - To grant financial aid to deserving students and to control work-study programs on campus.

Information Needs -

Requires the use of the student data base to access records in the performance of their duties. Cannot create or update any records in the student data base.

Scheduling

Interviewee - Thomas Chamberlain

Function - Prepare and maintain the schedule of all courses being given at the university.

Information Needs -

Has no access to the student data base. All work is done on their own data which is then provided to the registrar for registration purposes.

Institutional Studies

Interviewee - George Beatty

Function - To satisfy the needs of the university for statistical reports about the operation of the university.

Information Needs -

Has complete access to all student information for the purpose of completing their studies. Does not have the power to update or create records but can create certain statistical records as an intermediate step in the completion of their work.

Administrative Data Processing

Interviewee - Raymond Bombard
Malcolm Fiske

Function - To supply computer related services to all user groups in the university.

Information Needs -

Based on their function, they have access to all student records but do not have the authority to create or update records except when acting as an agent of a user.

Telephone

Function - To act as student telephone information service.

Information Needs -

Access to the student data base to obtain student name, student number, current phone number, and permanent phone number. Have no power to create or update information.

Public Safety

Function - Law enforcement of the university. Responsible for protecting the property of the university, its student body, and employees from illegal attack and the student body and employees from personal harm. Authorized to make arrests and investigations leading to arrest.

Information Needs -

Has access to various data elements in the student data base including student name, number, address and parent's name and address. No access to student grades or financial records.

APPENDIX B

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
I. BASIC CLASSIFICATION AND IDENTIFICATION DATA										
1. Student Number	X	X	X							
2 Social Security Number	X	X	X							
3 Student Name	X	X	X							
4 Level	X	X	X							
5 Class	X	X	X							
6 Half Year and Expiration			X							
7 Sex	X	X	X							
8 Maritial Status	X	X	X							
9 Date of Birth	X	X	X							
10 Veteran	X	X	X							
11 Citizenship/Visa	X	X	X							
12 CCEBS	X	X								
13 Religious Preference	X		X							
14 Ethnic-origin	X	X	X							
15 Major Department Title	X	X	X							
16 Major Departmtne Number	X	X	X							
17 Fraternity/Sorority	X									
II. PARENT/GUARDIAN AND PERMANENT NAME AND ADDRESS DATA										
18 Name of Parent/Guardian	X	X	X							
19 Address of Parent/Guardian	X	X	X							
20 Permanent Address	X	X	X							
21 Foreign Country	X	X	X							
22 Home Telephone	X	X	X							
23 Zip Code	X	X	X							

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
III. ENROLLMENT AND WITHDRAWAL DATA										
24 Entry Date	X	X	X							
25 Entrance Status	X	X	X							
26 Entrance Semester	X	X	X							
27 Latest Admissions Mode	X	X	X							
28 Latest Entrance Semester	X	X	X							
29 Initial Admissions Mode	X	X	X							
30 Initial Entrance Semester	X	X	X							
31 Initial Entrance Class	X	X	X							
32 Withdrawal Date	X		X							
33 Withdrawal Reason	X		X							
34 Semesters Complete										
35 Summer Withdrawal Date	X		X							
36 Previous Withdrawal Date										
37 Previous Withdrawal Reason										
38 Previous Number Semesters Completed										
39 Initial Withdrawal Date	X		X							
40 Initial Withdrawal Reason	X		X							
41 Initial Number Semesters Completed	X		X							
42 Future Withdrawal Reason										
43 Future Number Semesters Completed										
44 Date Withdrawal Notice										
46 Withdrawal Effective										
47 Withdrawal Processed					X					
48 Summer Session Codes	X									

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
IV. LOCAL (ON CAMPUS) RESIDENCE INFORMATION--CURRENT										
49 School Address					X					
50 School Telephone					X					
51 Residence Area					X					
52 Residence Hall Space Code					X					
53 Residence Hall Building Project Code					X					
54 No Address Flag					X					
55 On Exchange Flag					X					
56 Exchange Program					X					
V. LOCAL (ON CAMPUS) RESIDENCE INFORMATION--FUTURE										
57 School Address					X					
58 School Telephone					X					
59 Residence Area					X					
60 Residence Hall Space Code					X					
61 Residence Hall Building Project Code					X					
62 No Address Flag					X					
63 On Exchange Flag					X					
64 Not Returning Flag					X					
VI. MISCELLANEOUS BILLING DATA										
65 Billing Residence Category				X						
66 Latest Semester Billed				X						
67 Fee Paid/Cleared Code				X						
68 Alternate Address Code				X						
69 Campus Residence Regulations Exception Flag				X						

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
70 Board Regulation Exemption				X						
71 Coed Permission Code				X						
72 Room Deposit Paid Flag				X						
73 Amount of Room Deposit				X						
74 Graduate Billing Block				X						
75 Clearance Cards Made Flag				X						
76 Board Paid/Cleared				X						
VII. ACADEMIC DATA										
77 Credit/Point Data	X		X							
78 Degree Credits	X		X							
79 Required Degree Subjects Record	X		X							
80 Last Semester Completed	X		X							
81 Semester Status Flag										
82 Probation Counter										
83 Suspensions										
84 Graduation Diploma Name	X		X							
85 Expected Degree	X		X							
86 Expected Degree Date	X		X							
87 Registrar's Degree Clearance Flag	X		X							
88 Department/School Degree Clearance Flag	X		X							
89 No Honors Flag	X		X							
90 Number Credits Passed										
91 Number Credits Graded										
92 Number Pass/Fail Core										

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
93 Number Credits Pass/Fail										
94 Number Semesters Completed										
95 Pre-Registration Flag										
96 Schedule Change Flag										
VIII. ADMISSIONS DATA										
97 Admissions Update Code		X	X							
98 Last Institution Code		X	X							
99 Admissions Data		X								
100 Graduate Admissions Data			X							
101 Summer Counseling Session		X								
IX. MISCELLANEOUS PROCESSING DATA										
102 Teleprocessing Flags										
103 Comment Lines	X		X							
104 TP Change Printed Flag										
105 National Defence Code			X	X						
106 Health Form on File Flag	X		X							
107 Delete Flag	X	X	X							
108 Print Flag										
X. FEES										
109 Tution				X						
110 Graduate Tax				X						
111 Undergraduate Tax				X						
112 Health Fee				X						
113 Medical Insurance				X						

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
114 Identification Card				X						
115 Board				X						
116 Rent				X						
117 Telephone				X						
118 Campus Center				X						
119 Fine Arts				X						
120 Program Fee				X						
121 WMMASS PIRG				X						
122 Late Registration				X						
123 Graduation Fee				X						

APPENDIX C

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies	
I. BASIC CLASSIFICATION AND IDENTIFICATION DATA											
1. Student Number	1	1	1	1	1	1	1	1	1	1	
2 Social Security Number	1	1	1	1	1	1	0	0	0	1	
3 Student Name	1	1	1	1	1	1	1	1	1	1	
4 Level	1	1	1	1	1	1	1	1	1	1	
5 Class	1	1	1	1	1	1	0	1	0	1	
6 Half Year and Expiration	1	1	1	1	1	1	0	0	0	1	
7 Sex	1	1	1	1	1	1	0	1	1	1	
8 Maritial Status	1	1	1	1	1	1	0	1	0	1	
9 Date of Birth	1	1	1	1	1	1	0	1	0	1	
10 Veteran	1	1	1	1	1	1	0	1	0	1	
11 Citizenship/Visa	1	1	1	1	1	1	0	1	0	1	
12 CCEBS	1	1	1	1	1	1	0	1	0	1	
13 Religious Preference	1	1	1	0	0	0	0	0	0	1	
14 Ethnic-origin	1	1	1	1	1	1	0	0	0	1	
15 Major Department Title	1	1	1	1	0	1	0	0	0	1	
16 Major Departmtne Number	1	1	1	1	0	1	0	0	0	1	
17 Fraternity/Sorority	1	1	1	1	1	1	0	0	0	1	
II. PARENT/GUARDIAN AND PERMANENT NAME AND ADDRESS DATA											
18 Name of Parent/Guardian	1	1	1	1	0	1	0	0	0	1	
19 Address of Parent/Guardian	1	1	1	1	0	1	0	0	0	1	
20 Permanent Address	1	1	1	1	0	1	0	0	0	1	
21 Foreign Country	1	1	1	1	0	1	0	0	0	1	
22 Home Telephone	1	1	1	1	0	1	0	0	0	1	
23 Zip Code	1	1	1	1	0	1	0	0	0	1	

III. ENROLLMENT AND WITHDRAWAL DATA	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
24 Entry Date	1	1	1	1	1	1	0	0	0	1
25 Entrance Status	1	1	1	1	1	1	0	0	0	1
26 Entrance Semester	1	1	1	1	1	1	0	0	0	1
27 Latest Admissions Mode	1	1	1	1	1	1	0	0	0	1
28 Latest Entrance Semester	1	1	1	1	1	1	0	0	0	1
29 Initial Admissions Mode	1	1	1	1	1	1	0	0	0	1
30 Initial Entrance Semester	1	1	1	1	1	1	0	0	0	1
31 Initial Entrance Class	1	1	1	1	1	1	0	0	0	1
32 Withdrawal Date	1	1	1	1	1	1	0	0	0	1
33 Withdrawal Reason	1	1	1	1	1	1	0	0	0	1
34 Semesters Complete	1	1	1	1	1	1	0	0	0	1
35 Summer Withdrawal Date	1	1	1	1	1	1	0	0	0	1
36 Previous Withdrawal Date	1	1	1	1	1	1	0	0	0	1
37 Previous Withdrawal Reason	1	1	1	1	1	1	0	0	0	1
38 Previous Number Semesters Completed	1	1	1	1	1	1	0	0	0	1
39 Initial Withdrawal Date	1	1	1	1	1	1	0	0	0	1
40 Initial Withdrawal Reason	1	1	1	1	1	1	0	0	0	1
41 Initial Number Semesters Completed	1	1	1	1	1	1	0	0	0	1
42 Future Withdrawal Reason	1	1	1	1	1	1	0	0	0	1
43 Future Number Semesters Completed	1	1	1	1	1	1	0	0	0	1
44 Date Withdrawal Notice	1	1	1	1	1	1	0	0	0	1
46 Withdrawal Effective	1	1	1	1	1	1	0	0	0	1
47 Withdrawal Processed	1	1	1	1	1	1	0	0	0	1
48 Summer Session Codes	1	1	1	1	1	1	0	0	0	1

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
IV. LOCAL (ON CAMPUS) RESIDENCE INFORMATION--CURRENT										
49 School Address	1	0	1	1	1	1	0	0	0	1
50 School Telephone	1	0	1	1	1	1	1	0	0	1
51 Residence Area	1	0	1	1	1	1	0	0	0	1
52 Residence Hall Space Code	1	0	1	1	1	1	0	0	0	1
53 Residence Hall Building Project Code	1	0	1	1	1	1	0	0	0	1
54 No Address Flag	1	0	1	1	1	1	0	0	0	1
55 On Exchange Flag	1	0	0	1	1	1	0	0	0	1
56 Exchange Program	1	0	0	1	1	1	0	0	0	1
V. LOCAL (ON CAMPUS) RESIDENCE INFORMATION--FUTURE										
57 School Address	1	0	1	1	1	1	0	0	0	1
58 School Telephone	1	0	1	1	1	1	0	0	0	1
59 Residence Area	1	0	1	1	1	1	0	0	0	1
60 Residence Hall Space Code	1	0	1	1	1	1	0	0	0	1
61 Residence Hall Building Project Code	1	0	1	1	1	1	0	0	0	1
62 No Address Flag	1	0	1	1	1	1	0	0	0	1
63 On Exchange Flag	1	0	1	1	1	1	0	0	0	1
64 Not Returning Flag	1	0	1	1	1	1	0	0	0	1
VI. MISCELLANEOUS BILLING DATA										
65 Billing Residence Category	1	0	1	1	1	1	0	0	0	1
66 Latest Semester Billed	1	0	1	1	1	1	0	0	0	1
67 Fee Paid/Cleared Code	1	0	1	1	1	1	0	0	0	1
68 Alternate Address Code	1	0	1	1	1	1	0	0	0	1
69 Campus Residence Regulations Exception Flag	1	0	0	1	1	1	0	0	0	1

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
70 Board Regulation Exemption	1	0	0	1	1	1	0	0	0	1
71 Coed Permission Code	1	0	1	1	1	1	0	0	0	1
72 Room Deposit Paid Flag	1	0	1	1	1	1	0	0	0	1
73 Amount of Room Deposit	1	0	1	1	1	1	0	0	0	1
74 Graduate Billing Block	0	0	1	1	1	1	0	0	0	1
75 Clearance Cards Made Flag	1	0	1	1	1	1	0	0	0	1
76 Board Paid/Cleared	1	0	1	1	1	1	0	0	0	1
VII. ACADEMIC DATA										
77 Credit/Point Data	1	0	1	1	0	1	0	0	0	1
78 Degree Credits	1	0	1	1	0	1	0	0	0	1
79 Required Degree Subjects Record	1	0	1	1	0	1	0	0	0	1
80 Last Semester Completed	1	0	1	1	0	1	0	0	0	1
81 Semester Status Flag	1	0	1	1	0	1	0	0	0	1
82 Probation Counter	1	0	1	1	0	1	0	0	0	1
83 Suspensions	1	0	1	1	0	1	0	0	0	1
84 Graduation Diploma Name	1	0	1	1	0	1	0	0	0	1
85 Expected Degree	1	0	1	1	0	1	0	0	0	1
86 Expected Degree Date	1	0	1	1	0	1	0	0	0	1
87 Registrar's Degree Clearance Flag	1	0	1	1	0	1	0	0	0	1
88 Department/School Degree Clearance Flag	1	0	1	1	0	1	0	0	0	1
89 No Honors Flag	1	0	1	1	0	1	0	0	0	1
90 Number Credits Passed	1	0	1	1	0	1	0	0	0	1
91 Number Credits Graded	1	0	1	1	0	1	0	0	0	1
92 Number Pass/Fail Core	1	0	1	1	0	1	0	0	0	1

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
93 Number Credits Pass/Fail	1	0	1	1	0	1	0	0	0	1
94 Number Semesters Completed	1	0	1	1	0	1	0	0	0	1
95 Pre-Registration Flag	1	0	1	1	0	1	0	0	0	1
96 Schedule Change Flag	1	0	1	1	0	1	0	0	0	1
VIII. ADMISSIONS DATA										
97 Admissions Update Code	0	1	1	0	0	0	0	0	0	1
98 Last Institution Code	0	1	1	0	0	0	0	0	0	1
99 Admissions Data	0	1	0	1	0	0	0	0	0	1
100 Graduate Admissions Data	0	0	1	1	0	0	0	0	0	1
101 Summer Counseling Session	0	1	0	1	0	0	0	0	0	1
IX. MISCELLANEOUS PROCESSING DATA										
102 Teleprocessing Flags	0	0	0	0	0	0	0	0	0	0
103 Comment Lines	1	0	1	0	0	0	0	0	0	0
104 TP Change Printed Flag	0	0	0	0	0	0	0	0	0	0
105 National Defence Code	0	0	0	1	0	0	0	0	0	0
106 Health Form on File Flag	0	0	0	0	0	0	0	0	0	0
107 Delete Flag	1	0	1	0	1	0	0	0	0	0
108 Print Flag	0	0	0	0	0	0	0	0	0	0
X. FEES										
109 Tution	0	1	1	1	0	1	0	0	0	1
110 Graduate Tax	0	0	1	1	0	0	0	0	0	1
111 Undergraduate Tax	0	0	0	1	0	0	0	0	0	1
112 Health Fee	0	0	0	1	0	0	0	0	0	1
113 Medical Insurance	0	0	0	1	0	0	0	0	0	1

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
114 Identification Card	0	0	1	1	0	0	0	0	0	1
115 Board	0	0	0	1	1	1	0	0	0	1
116 Rent	0	0	0	1	1	1	0	0	0	1
117 Telephone	0	0	0	1	0	0	0	0	0	1
118 Campus Center	0	0	0	1	0	0	0	0	0	1
119 Fine Arts	0	0	0	1	0	0	0	0	0	1
120 Program Fee	0	0	1	1	0	0	0	0	0	1
121 WMASS PIRG	0	0	0	1	0	0	0	0	0	1
122 Late Registration	1	0	0	1	0	0	0	0	0	1
123 Graduation Fee	1	0	0	1	0	0	0	0	0	1

APPENDIX D

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
I. BASIC CLASSIFICATION AND IDENTIFICATION DATA										
1. Student Number	1	1	1	0	0	0	0	0	0	0
2 Social Security Number	1	1	1	0	0	0	0	0	0	0
3 Student Name	1	1	1	0	0	0	0	0	0	0
4 Level	1	1	1	0	0	0	0	0	0	0
5 Class	1	1	1	0	0	0	0	0	0	0
6 Half Year and Expiration	0	0	1	0	0	0	0	0	0	0
7 Sex	1	1	1	0	0	0	0	0	0	0
8 Marital Status	1	1	1	0	0	0	0	0	0	0
9 Date of Birth	1	1	1	0	0	0	0	0	0	0
10 Veteran	1	1	1	0	0	0	0	0	0	0
11 Citizenship/Visa	1	1	1	0	0	0	0	0	0	0
12 CCEBS	1	1	1	0	0	0	0	0	0	0
13 Religious Preference	1	0	1	0	0	0	0	0	0	0
14 Ethnic-origin	1	1	1	0	0	0	0	0	0	0
15 Major Department Title	1	1	1	0	0	0	0	0	0	0
16 Major Departmtne Number	1	1	1	0	0	0	0	0	0	0
17 Fraternity/Sorority	1	0	1	0	0	0	0	0	0	0
II. PARENT/GUARDIAN AND PERMANENT NAME AND ADDRESS DATA										
18 Name of Parent/Guardian	1	1	1	0	0	0	0	0	0	0
19 Address of Parent/Guardian	1	1	1	0	0	0	0	0	0	0
20 Permanent Address	1	1	1	0	0	0	0	0	0	0
21 Foreign Country	1	1	1	0	0	0	0	0	0	0
22 Home Telephone	1	1	1	0	0	0	0	0	0	0
23 Zip Code	1	1	1	0	0	0	0	0	0	0

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
III. ENROLLMENT AND WITHDRAWAL DATA										
24 Entry Date	1	1	1	0	0	0	0	0	0	0
25 Entrance Status	1	1	1	0	0	0	0	0	0	0
26 Entrance Semester	1	1	1	0	0	0	0	0	0	0
27 Latest Admissions Mode	1	1	1	0	0	0	0	0	0	0
28 Latest Entrance Semester	1	1	1	0	0	0	0	0	0	0
29 Initial Admissions Mode	1	1	1	0	0	0	0	0	0	0
30 Initial Entrance Semester	1	1	1	0	0	0	0	0	0	0
31 Initial Entrance Class	1	1	1	0	0	0	0	0	0	0
32 Withdrawal Date	1	0	1	0	0	0	0	0	0	0
33 Withdrawal Reason	1	0	1	0	0	0	0	0	0	0
34 Semesters Complete	1	0	1	0	0	0	0	0	0	0
35 Summer Withdrawal Date	1	0	1	0	0	0	0	0	0	0
36 Previous Withdrawal Date	1	0	1	0	0	0	0	0	0	0
37 Previous Withdrawal Reason	1	0	1	0	0	0	0	0	0	0
38 Previous Furber Semesters Completed	1	0	1	0	0	0	0	0	0	0
39 Initial Withdrawal Date	1	0	1	0	0	0	0	0	0	0
40 Initial Withdrawal Reason	1	0	1	0	0	0	0	0	0	0
41 Initial Number Semesters Completed	1	0	1	0	0	0	0	0	0	0
42 Future Withdrawal Reason	1	0	1	0	0	0	0	0	0	0
43 Future Number Semesters Completed	1	0	1	0	0	0	0	0	0	0
44 Date Withdrawal Notice	1	0	1	0	0	0	0	0	0	0
46 Withdrawal Effective	1	0	1	0	0	0	0	0	0	0
47 Withdrawal Processed	1	0	1	0	0	0	0	0	0	0
48 Summer Session Codes	1	0	0	0	0	0	0	0	0	0

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
IV. LOCAL (ON CAMPUS) RESIDENCE INFORMATION--CURRENT										
49 School Address	1	0	1	0	1	0	0	0	0	0
50 School Telephone	1	0	1	0	1	0	0	0	0	0
51 Residence Area	1	0	1	0	1	0	0	0	0	0
52 Residence Hall Space Code	1	0	1	0	1	0	0	0	0	0
53 Residence Hall Building Project Code	1	0	1	0	1	0	0	0	0	0
54 No Address Flag	1	0	1	0	1	0	0	0	0	0
55 On Exchange Flag	1	0	0	0	1	0	0	0	0	0
56 Exchange Program	1	0	0	0	1	0	0	0	0	0
V. LOCAL (ON CAMPUS) RESIDENCE INFORMATION--FUTURE										
57 School Address	1	0	0	0	1	0	0	0	0	0
58 School Telephone	1	0	0	0	1	0	0	0	0	0
59 Residence Area	1	0	0	0	1	0	0	0	0	0
60 Residence Hall Space Code	1	0	0	0	1	0	0	0	0	0
61 Residence Hall Building Project Code	1	0	0	0	1	0	0	0	0	0
62 No Address Flag	1	0	0	0	1	0	0	0	0	0
63 On Exchange Flag	1	0	0	0	1	0	0	0	0	0
64 Not Returning Flag	1	0	0	0	1	0	0	0	0	0
VI. MISCELLANEOUS BILLING DATA										
65 Billing Residence Category	0	0	0	1	0	0	0	0	0	0
66 Latest Semester Billed	0	0	0	1	0	0	0	0	0	0
67 Fee Paid/Cleared Code	0	0	0	1	0	0	0	0	0	0
68 Alternate Address Code	0	0	0	1	0	0	0	0	0	0
69 Campus Residence Regulations Exception Flag	0	0	0	1	0	0	0	0	0	0

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
70 Board Regulation Exemption	0	0	0	1	0	0	0	0	0	0
71 Coed Permission Code	0	0	0	1	0	0	0	0	0	0
72 Room Deposit Paid Flag	0	0	0	1	0	0	0	0	0	0
73 Amount of Room Deposit	0	0	0	1	0	0	0	0	0	0
74 Graduate Billing Block	0	0	0	1	0	0	0	0	0	0
75 Clearance Cards Made Flag	0	0	0	1	0	0	0	0	0	0
76 Board Paid/Cleared	0	0	0	1	0	0	0	0	0	0
VII. ACADEMIC DATA										
77 Credit/Point Data	1	0	1	0	0	0	0	0	0	0
78 Degree Credits	1	0	1	0	0	0	0	0	0	0
79 Required Degree Subjects Record	1	0	1	0	0	0	0	0	0	0
80 Last Semester Completed	1	0	1	0	0	0	0	0	0	0
81 Semester Status Flag	0	0	0	0	0	0	0	0	0	0
82 Probation Counter	0	0	0	0	0	0	0	0	0	0
83 Suspensions	0	0	0	0	0	0	0	0	0	0
84 Graduation Diploma Name	1	0	1	0	0	0	0	0	0	0
85 Expected Degree	1	0	1	0	0	0	0	0	0	0
86 Expected Degree Date	1	0	1	0	0	0	0	0	0	0
87 Registrar's Degree Clearance Flag	1	0	1	0	0	0	0	0	0	0
88 Department/School Degree Clearance Flag	1	0	1	0	0	0	0	0	0	0
89 No Honors Flag	1	0	1	0	0	0	0	0	0	0
90 Number Credits Passed	1	0	1	0	0	0	0	0	0	0
91 Number Credits Graded	1	0	1	0	0	0	0	0	0	0
92 Number Pass/Fail Core	1	0	1	0	0	0	0	0	0	0

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
93 Number Credits Pass/Fail	1	0	1	0	0	0	0	0	0	0
94 Number Semesters Completed	1	0	1	0	0	0	0	0	0	0
95 Pre-Registration Flag	1	0	1	0	0	0	0	0	0	0
96 Schedule Change Flag	1	0	1	0	0	0	0	0	0	0
VIII. ADMISSIONS DATA										
97 Admissions Update Code	0	1	1	0	0	0	0	0	0	0
98 Last Institution Code	0	1	1	0	0	0	0	0	0	0
99 Admissions Data	0	1	0	0	0	0	0	0	0	0
100 Graduate Admissions Data	0	0	1	0	0	0	0	0	0	0
101 Summer Counseling Session	0	1	0	0	0	0	0	0	0	0
IX. MISCELLANEOUS PROCESSING DATA										
102 Teleprocessing Flags	0	0	0	0	0	0	0	0	0	0
103 Comment Lines	0	0	0	0	0	0	0	0	0	0
104 TP Change Printed Flag	0	0	0	0	0	0	0	0	0	0
105 National Defence Code	0	0	0	1	0	1	0	0	0	0
106 Health Form on File Flag	1	0	0	0	0	0	0	0	0	0
107 Delete Flag	0	0	0	0	0	0	0	0	0	0
108 Print Flag	0	0	0	0	0	0	0	0	0	0
X. FEES										
109 Tution	0	0	0	1	0	0	0	0	0	0
110 Graduate Tax	0	0	0	1	0	0	0	0	0	0
111 Undergraduate Tax	0	0	0	1	0	0	0	0	0	0
112 Health Fee	0	0	0	1	0	0	0	0	0	0
113 Medical Insurance	0	0	0	1	0	0	0	0	0	0

	Registrar	Admissions	Graduate School	Bursar	Housing	Financial Aid	Telephone	Provost	Public Safety	Institutional Studies
114 Identification Card	0	0	0	1	0	0	0	0	0	0
115 Board	0	0	0	1	0	0	0	0	0	0
116 Rent	0	0	0	1	0	0	0	0	0	0
117 Telephone	0	0	0	1	0	0	0	0	0	0
118 Campus Center	0	0	0	1	0	0	0	0	0	0
119 Fine Arts	0	0	0	1	0	0	0	0	0	0
120 Program Fee	0	0	0	1	0	0	0	0	0	0
121 WMMASS PIRG	0	0	0	1	0	0	0	0	0	0
122 Late Registration	0	0	0	1	0	0	0	0	0	0
123 Graduation Fee	0	0	0	1	0	0	0	0	0	0

APPENDIX E

APPENDIX E

DATA ELEMENT	FREQUENCY OF USE	DATA ELEMENT	FREQUENCY OF USE
1	115	55	25
2	31	57	47
3	93	58	13
4	116	59	6
5	91	60	4
6	12	61	27
7	50	62	6
8	36	63	18
9	35	64	8
10	47	67	13
11	29	68	8
12	24	69	27
13	27	70	7
14	25	71	4
15	54	72	17
16	1	73	11
17	9	75	15
18	17	76	1
19	60	77	78
20	209	78	36
21	16	79	197
22	17	80	8
24	19	82	4
26	48	83	4
32	84	85	25
33	28	86	21
34	11	87	13
35	13	88	8
37	8	89	6
38	6	90	5
39	15	91	6
40	6	92	4
41	5	93	5
42	12	95	7
43	7	98	13
44	7	99	73
45	8	100	34
47	1	101	1
48	1	102	5
49	165	103	15
50	26	105	4
51	9	106	1
52	5	108	10
53	10	115	4
54	6	116	37

120	11
201	3
202	189
203	141
204	41
205	23
206	17
207	33
208	6
209	2
210	1
211	4
212	7
213	4
999	20

APPENDIX F

APPENDIX F

DATA ELEMENT	FREQUENCY OF USE	DATA ELEMENT	FREQUENCY OF USE
20	209	21	16
79	107	75	15
202	189	103	15
49	165	39	15
203	141	87	13
4	116	58	13
1	115	35	13
3	93	67	13
5	91	98	13
32	84	42	12
77	78	6	12
99	73	120	11
19	60	34	11
15	54	73	11
7	50	53	10
26	48	103	10
10	47	51	9
57	47	17	9
204	41	68	8
116	37	88	8
8	36	45	8
78	36	64	8
9	35	37	8
100	34	80	8
207	33	43	7
2	31	95	7
11	29	44	7
33	28	70	7
61	27	212	7
69	27	208	6
13	27	54	6
50	26	40	6
14	25	62	6
85	25	59	6
55	25	89	6
12	24	38	6
205	23	91	6
86	21	52	5
999	20	41	5
24	19	90	5
63	18	93	5
18	17	102	5
22	17	115	4
72	17	60	4
206	17	211	4

105	4
92	4
82	4
83	4
71	4
213	4
201	3
209	2
76	1
218	1
106	1
16	1
101	1
48	1
47	1