Security in Automatic Data Processing Systems

1976

Eduardo G. Mendez

University of Central Florida

Find similar works at: https://stars.library.ucf.edu/rtd

University of Central Florida Libraries http://library.ucf.edu

Part of the Engineering Commons

STARS Citation


This Masters Thesis (Open Access) is brought to you for free and open access by STARS. It has been accepted for inclusion in Retrospective Theses and Dissertations by an authorized administrator of STARS. For more information, please contact lee.dotson@ucf.edu.
SECURITY IN AUTOMATIC DATA PROCESSING SYSTEMS

BY

EDUARDO G. MENDEZ
A.A., MIAMI-DADE COMMUNITY COLLEGE
B.S., UNIVERSITY OF WEST-FLORIDA

RESEARCH REPORT

Submitted in partial fulfillment of the requirements for the degree of Master of Science in the Graduate Studies Program of the College of Engineering Florida Technological University

Orlando, Florida
1976
ACKNOWLEDGEMENTS

The author gratefully acknowledges the understanding, encouragement and aid given by his wife Yolanda and his parents Rodolfo and Ana Maria Mendez during all of his educational endeavors. He is also very thankful to the Industrial Engineering and Management Systems faculty for the advice and guidance given throughout his academic work at Florida Technological University.
SECURITY IN AUTOMATIC DATA PROCESSING SYSTEMS

ABSTRACT

Security in automatic data processing systems is concerned with the protection of equipment and data against unauthorized modifications or destruction, and accidental or intentional disclosure of information.

This report consists of two parts:

1. An overview of current literature in the field. In this part, basic problems and solutions, terminology and concepts found in the theoretical aspects of data processing systems security are described.

2. A survey of the state of the art in a sample area. During the survey, information about actual applications of security methods in the Orlando, Florida area was collected. This information was gathered by means of a questionnaire and it will permit a comparative analysis between the usage of security measures in large and small firms.

It is hoped that this study will provide valuable information to both the computer practitioner and management and in addition, will create an awareness of the important role that the security function plays in an organization.

[Signature]
Director of Research Report
TABLE OF CONTENTS

ACKNOWLEDGMENTS .................................................. iii
ABSTRACT ........................................................................ iv
INTRODUCTION ............................................................ 1

Chapter

I. OBJECTIVES, SCOPE AND PROCEDURE ......................... 10
II. STATEMENT OF THE PROBLEM .................................. 12
III. DEFINITION OF A FEW GENERAL TERMS .................... 19
IV. THE STUDY AND RESULTS .......................................... 22
   A. Introduction and Basic Framework ............................. 22
   B. Personnel Section .................................................. 24
      Statement of the Problem
      General Guidelines
      Description of the Questionnaire
      Comparison of Responses
      Analysis of Responses
   C. Physical Section ..................................................... 30
      Statement of the Problem
      General Guidelines
      Description of the Questionnaire
      Comparison of Responses
      Analysis of Responses
   D. Data, Programs and Documentation Section ............... 44
      Statement of the Problem
      General Guidelines
      Description of the Questionnaire
      Comparison of Responses
      Analysis of Responses
   E. Backup Section ....................................................... 53
      Statement of the Problem
      General Guidelines
      Description of the Questionnaire
      Comparison of Responses
      Analysis of Response
<table>
<thead>
<tr>
<th>F. Development Section</th>
<th>59</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statement of the Problem</td>
<td>59</td>
</tr>
<tr>
<td>General Guidelines</td>
<td>59</td>
</tr>
<tr>
<td>Description of the Questionnaire</td>
<td>59</td>
</tr>
<tr>
<td>Comparison of Responses</td>
<td>59</td>
</tr>
<tr>
<td>Analysis of Responses</td>
<td>59</td>
</tr>
<tr>
<td>V. CONCLUSIONS</td>
<td>66</td>
</tr>
<tr>
<td>APPENDIX</td>
<td>69</td>
</tr>
<tr>
<td>BIBLIOGRAPHY</td>
<td>80</td>
</tr>
</tbody>
</table>
LIST OF TABLES

1. Electronic and Accounting Equipment: Projections ................. 2
2. Computer Related Crimes 1964-1972 .................. 7
3. Types of Security Exposure ....................... 15
4. Personnel Section - Comparison of Responses ........ 28
5. Physical Section - Comparison of Responses .......... 42
6. Data, Programs and Documentation Section - Comparison of Responses .......... 49
7. Backup Section - Comparison of Responses ......... 57
8. Development Section - Comparison of Responses ..... 63
LIST OF ILLUSTRATIONS

Figure

1. Installed Dollars in Computing Equipment 1967-73 3
2. Crime Clocks 1973 4
5. Threats and Their Usual Defense 17
6. Sources of Computer Errors 18
7. Threats and Countermeasures 31
8. Summary of Results - Personnel Section Large Organizations 70
9. Summary of Results - Personnel Section Small Organizations 71
10. Summary of Results - Physical Section Large Organizations 72
11. Summary of Results - Physical Section Small Organizations 73
12. Summary of Results - Data Programs and Documentation Section - Large Organizations 74
13. Summary of Results - Data Programs and Documentation Section - Small Organizations 75
14. Summary of Results - Backup Section Large Organizations 76
15. Summary of Results - Backup Section Small Organizations 77
16. Summary of Results - Development Large Organizations 78
17. Summary of Results - Development Small Organizations 79
INTRODUCTION

The use of computer systems has grown to the extent that they have become a critical and indispensable resource in today's society.

There is a widespread use of automatic data processing technology by a large number of organizations.

Some examples of computer users are: The Department of Defense, The Internal Revenue Service, The Federal Bureau of Investigation, the banking industry, insurance companies, health institutions, colleges and universities, manufacturing and retailing businesses.

The demand for computer systems is growing rapidly as new technological advances permit the marketing of a large variety of electronic processing equipment. Some facts on this growth are shown on Table 1 and Figure 1.

In addition to the increase in computer utilization, there has been an increase in crime in our society. The cost of 'ordinary' crimes against business had reached $23.6 billion in 1975. (U. S. Department of Justice. Federal Bureau of Investigation. 1973, p.7). Crime can affect businesses regardless of location, although the incidence varies by the type of area. The growth of crime is described in Figures 2, 3 and 4.
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3573</td>
<td>Computers &amp; Related Equipment</td>
<td>5,965</td>
<td>6,740</td>
<td>10,450</td>
<td>12,100</td>
<td>13,746</td>
<td>22,560</td>
</tr>
<tr>
<td>3574</td>
<td>Calculating and Accounting Machines</td>
<td>588</td>
<td>647</td>
<td>1,110</td>
<td>1,335</td>
<td>---</td>
<td>3,450</td>
</tr>
</tbody>
</table>


Fig. 1. Installed Dollars In Computing Equipment 1967-1973

SERIOUS CRIMES
16 EACH MINUTE

VIOLENT CRIMES
MURDER, FORCIBLE RAPE, ROBBERY OR ASSAULT TO KILL
ONE EVERY 36 SECONDS

MURDER
ONE EVERY 27 MINUTES

FORCIBLE RAPE
ONE EVERY 10 MINUTES

AGGRAVATED ASSAULT
ONE EVERY 76 SECONDS

ROBBERY
ONE EVERY 82 SECONDS

BURGLARY
ONE EVERY 12 SECONDS

LARCENY-THEFT
ONE EVERY 7 SECONDS

AUTO THEFT
ONE EVERY 34 SECONDS

Fig. 2. Crime Clocks 1973

Fig. 3. Crime and Population 1968-1973.

CRIMES AGAINST PROPERTY
1968-1973
PERCENT CHANGE OVER 1966
LIMITED TO BURGLARY, LARCENY-THEFT AND AUTO THEFT

Fig. 4. Crime Against Property 1968-1973.

This high level and variety of crime could not leave the field of computer applications untouched. A number of incidents involving automated information systems is found in Table 2.

**TABLE 2**

**COMPUTER RELATED CRIMES**

1964-1972

<table>
<thead>
<tr>
<th>Category of Incident</th>
<th>No. of Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sabotage</td>
<td>15</td>
</tr>
<tr>
<td>Theft</td>
<td>23</td>
</tr>
<tr>
<td>Copying (Data)</td>
<td>8</td>
</tr>
<tr>
<td>Tampering</td>
<td>23</td>
</tr>
<tr>
<td>Masquerading</td>
<td>2</td>
</tr>
<tr>
<td>Fraudulent Activities</td>
<td>5, 76</td>
</tr>
</tbody>
</table>


If the three factors discussed above (increasing computer usage, crime and computer related incidents) are considered and analyzed, it can be easily concluded that the need for security in data and computer systems has become increasingly important.

The evolution of the computer from a laboratory curiosity, to a prestigious luxury, to a vitally necessary administrative tool
has brought with it many problems in the areas of security, accuracy and privacy.

The problem of computer security has also been changing in nature. Early systems could have been provided with a large degree of protection by strict physical security procedures. The computer could have been made basically secure by virtue of the fact that the entire system could have been placed behind a well guarded wall, thereby restricting access to the machine for input and output with relative ease.

As computer systems have grown more sophisticated and varied, and time-sharing operation, telecommunications, multiprogramming, and mass-storage devices have become available, new security procedures have been needed. However, it is not enough to simply furnish security measures. Measures should not only minimize risk and probability of loss, but should be available at a reasonable cost.

Important decisions about costs and risks must now be faced by management and it must become aware of the general problems and solutions of the data processing security areas.

A trade-off between the degree of protection and cost is now essential in that a great deal of computer security can be provided with today's technology but only at a significant cost.
Management should understand the basic concepts and threats to the information processing system in order to approve and direct the implementation of security procedures.
CHAPTER I

OBJECTIVES, SCOPE AND PROCEDURE

The objectives of this report are:

1. To acquaint the reader with some basic concepts and terms found in the field of computer security.
2. To describe the most common threats to electronic data processing applications.
3. To present a set of basic general solutions available to countermand the possible threats.
4. To discuss the weaknesses found in existing firms and recommend possible solutions.

The scope of the report will be limited to five areas of analysis: personnel, physical, backup, development, and data programs and documentation. Within each one of these areas the following will be discussed; general security problems, general guidelines (or procedures), the questionnaire used for the survey, the results obtained and an analysis of those results.

The procedure followed to accomplish the proposed objectives consists of two parts:

1. An overview of current literature in the computer and data security area. From this study, basic concepts, threats and general guidelines are obtained for later discussion.
2. A survey of actual applications of security methods was performed. This information was gathered by means of a questionnaire and it will permit a comparative analysis between the usage of computer security procedures in large and small firms.
CHAPTER II

STATEMENT OF THE PROBLEM

The desired end product of the four objectives stated in Chapter I is a set of countermeasures that will permit the proper functioning of the data processing system.

Proper functioning is defined as the satisfactory completion of all necessary and desirable functions of the data processing application.

The applications should be performed without the loss of any data, the introduction of errors, or permitting data to be read or modified with no authorization.

To accomplish the desired level of functioning, a variety of preventive, protective, recovery and detection procedures should be applied. These are the types of measures that will be discussed in this report.

The need for these various measures can be summarized as follows:

a) The probability of a hazardous event happening at all should be minimized and the actions taken should be preventive.

b) Controls should be designated to detect and minimize the damage of threat if it does occur.

The preventive actions will not always work,
therefore, it is necessary to protect the personnel, hardware and software from the harm that could result.

c) Designing a method of recovery from damage is vital to the overall security plan. If damage has occurred, there must be plans to make a quick recovery possible.

It is the responsibility of management to concern itself with the safeguarding of resources under its jurisdiction, and to organize, control and direct both human and capital resources.

It is important to recognize that there are no simple formulas for examining the cost-value trade-offs in applying data security measures.

The security procedures for any given system or installation are unique to its specific needs. There is not a prescribed set of rules that can guarantee complete security for all conditions.

The decision to implement any given set of data security techniques must be related to the degree of vulnerability of the computer, the value of the data in question, the policy guidelines and "atmosphere of concern" provided by general management.

Types of security exposure organized under six classifications (Acts of God, hardware and program failures, human carelessness, malicious damage, crime and invasion of privacy) are presented in Table 3. This type of table is an example that can be used to define the different types of threats to which the computer system
may be exposed.

A graphical description of the interrelationships between threats and lines of defense is presented in Figure 5. The nucleus of the methodology for control of security and accuracy lies in the design of the computer system and its programs, but it is important to consider that a set of layers of control are necessary to improve the protection against different types of threats.

It is common to hear or read stories about computers making phenomenal and sometimes pitiful errors. A brief presentation of the seven most common causes of errors may be found in Figure 6.

To maintain accuracy and security in a computer system the rate of errors must be minimized.

It is extremely important to recognize the possible threats and estimate the probability of occurrence in order to design the necessary countermeasures.
## TABLE 3

### TYPES OF SECURITY EXPOSURE

<table>
<thead>
<tr>
<th>Category</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ACTS OF GOD</strong></td>
<td>Fire, Flood, Act of War, Other Catastrophe</td>
</tr>
<tr>
<td><strong>HARDWARE AND PROGRAM FAILURES</strong></td>
<td>Computer outage, File unit damages disk track, Tape unit damages part of tape, Disk, or other volume, unreadable, Hardware/Software error damages file, Data Transmission error not detected, Card (or other input) chewed up by machine, Error in application program damages record</td>
</tr>
<tr>
<td><strong>HUMAN CARELESSNESS</strong></td>
<td>Keypunch errors, Terminal operator input error, Wrong volume mounted &amp; updated, Wrong version of program used, Accident during program testing, Mislaid tape or disk, Physical damage to tape of disk</td>
</tr>
<tr>
<td><strong>MALICIOUS DAMAGE</strong></td>
<td>Looting, Violent Sabotage, Nonviolent sabotage (e.g. tape erasure), Malicious computer operator</td>
</tr>
</tbody>
</table>
TABLE 3 - Continued

MALICIOUS DAMAGE - continued

Malicious programmer
Malicious tape librarian
Malicious terminal operator
Malicious user (e.g. punches holes in returnable card)
Playful malignancy (e.g. using terminal for fun)

CRIME

Embezzlement
Industrial espionage
Employees selling commercial secrets
Employees selling data for mailing lists
Data-bank information used for bribery or extortion

INVASION OF PRIVACY

Casual curiosity (e.g. salaries)
Looking up data for a competing corporation
Obtaining personal information for political or legal reasons
Nondeliberate revealing of private info
Malicious invasion of privacy

Fig. 5. Threats and Their Usual Defense.

HARDWARE ERRORS
Very infrequent. Hardware can be designed to detect virtually all its own errors.

SOFTWARE ERRORS
Especially in new software that has had little "field" testing. A nuisance but not a major cause of errors in output.

ERRORS IN APPLICATION PROGRAMS
The usual cause of wild behavior in a computer system. The cure: thorough program testing.

OPERATOR ERRORS
For example, an operator incorrectly recovering from a card jam or other failure. Solution: foolproof operating procedures.

DATA-INPUT ERRORS
"Garbage in: Garbage out. Cause: errors in keypunching, terminal entry or other manual input; use of wrong data. Necessary: keypunch verification, input controls, accuracy tests. Faulty input is the biggest cause of "computer errors".

INAPPROPRIATE PROGRAM DESIGN
Invalid decision-making process. Neglect of important parameters. For example: inappropriate method of setting overbooking limits in an airline may result in passengers being stranded at the airport.

QUESTIONABLE SYSTEM PHILOSOPHY
For example, the system is insufficiently flexible to handle unanticipated events; the system methodology imposes undesirable constraints on the operating environment; the effects of invalid data are acted upon without a double check (e.g., consumer's electricity is incorrectly cut off).

Fig. 6. Sources of Computer Errors

CHAPTER III

DEFINITION OF A FEW GENERAL TERMS

Before stating some of the most desirable conditions in a security program for an automatic data processing facility, it is important to define some basic concepts such as: security, privacy, confidentiality and anonymity.

1) Security refers to the protection against unauthorized disclosure, destruction or modification of (1) data, (2) software, (3) hardware, whether intentionally caused or resulting from accident or carelessness.

A brief description of what security means is given in Davis 1974, p. 21.

Data security is the protection of data against accidental disclosure or modification using both physical security measures and controlled accessibility. Physical security as it pertains to computers, does not differ from physical security for other installations. It is achieved through the use of locks, guards, badges, personnel security clearances and administratively controlled measures outside the computer as well as measures required for the protection of the structures housing the computer and related equipment against damage from accident, fire and environmental hazard, thus ensuring the protection of their contents.

Controlled accessibility is the set of technological measures of hardware and software available in a computer system for the protection of data.
2) Privacy relates to the rights of individuals and organizations to determine for themselves when, how and to what extent information about them is to be transmitted to others.

As stated in AFIPS Systems Review Manual on Security 1975, p.2.,

Privacy is therefore primarily a matter of an individual's personal concern with respect to information that may or may not be collected or divulged about himself or his affairs. Privacy is thus a matter of individual rights defined by public policy, court decisions, and legal statutes, ordinances, or regulations.

3) Confidentiality is a concept that deals with data, specifically it refers to the degree of protection which will be provided to minimize potential invasions of privacy.


Confidentiality involves relationships or agreements between the sources of information and the collectors, disseminators, or users of that information. It is a matter of protection of privacy (or of other constraints upon disclosure, distribution, or use of sensitive information). The area of confidentiality, rather than that of privacy per se, is thus the primary concern for system designers, systems managers, operators, users and evaluators.

4) Anonymity is a term which is described by Mosmann 1976, p. 170.

To attempt to hide publicly known facts, to remove or obscure such facts from the historical records (forget what has taken place in public, to erase the record, to decline to report).

Our anonymity has been protected when it has been protected at all - by inefficiencies of record keeping, and is attacked by efficiency and computer technology.
These general concepts implicitly suggest that any data processing mechanism (being it manually or automatically operated) needs some kind of protective measures. These set of protective measures imply a multistage problem that will be discussed in the next chapter.
CHAPTER IV

THE STUDY AND RESULTS

Introduction and Basic Framework

Although a prescription of specific security measures cannot be defined for all organizations, the literature in the field provides enough guidelines and information about security procedures to build a basic theoretical framework.

These general guidelines contain the type of technical measures that will tend to minimize the risk of violating the data integrity and security in data processing systems.

The basic structure is formed by five sections or important categories of control: Personnel, Physical, Backup, Development, and Data, Programs and Documentation. These general sections will be subdivided by specific areas of operation:

1. General Management
2. Exit Policies
3. Employee Identification
4. Vendor Hiring Policies
5. Hiring Policies
Discussions and analysis will be organized by subsections as presented above. The questionnaire used in the survey was designed to collect information about each of the areas of operation mentioned above and it is described in more detail in Tables 4, 5, 6, 7, and 8.

The survey consisted of eight companies (five small firms and three large ones) in the Orlando, Florida area. The prime criterion used to differentiate between small and large organizations was the total monthly rental for the computer system. A computer user who pays less than $10,000 per month for rental of the computer system is considered a small organization and vice versa if the user pays more than $10,000.

The questionnaire was filled out by means of personal interviews. The person being interviewed (Security officer or data
processing manager) in each case was asked to answer the questions as accurately as possible, it was also guaranteed that the identity of the company and the answers given will be kept completely confidential.

Personnel Section

Statement of The Problem

The basic protection of a data processing system begins with the integrity of people that have access to the hardware, software or handle any data.

A comment about the importance of personnel is found in AFIPS Systems Review Manual on Security 1975, p.12.

In the end, preservation of privacy rests not with machines but with men. The effectiveness of all protective measures, however sophisticated they may become, will still depend upon people: operators, service personnel, supervising officers, and all those who decide what information to put into a computer and how to use it.

The basic approach to maintain security in this area is to hire honest people, orient personnel on company's security procedures and design controls to minimize temptations.

General Guidelines

In order to maintain an acceptable level of control over personnel, the following measures are indispensable:

A. Personal and employment references, qualifications and skills of all applicants should be thoroughly checked.

B. Special orientation and training programs should be
provided where employees are found to be deficient in necessary qualifications and skills.

C. All employees should be thoroughly indoctrinated with the policies and practices of the organization, especially with respect to matters of confidentiality and security.

D. As small a number of people as possible should be entrusted with matters involving confidentiality and security.

E. Management should establish a protection program for employees against damage or injury, attack, and bribery or coercion. A safe environment must be engineered to assure the safety of the workforce.

F. Employees critically engaged in the handling or processing of sensitive or privileged information should be bonded, licensed, and/or certified.

G. Refresher sessions on security, confidentiality and protection of privacy should be held with all responsible personnel at regular periodic intervals.

H. Suspension and termination procedures must be carefully designed and conscientiously applied.

I. Supervisors should maintain close and effective communications with their staffs. They should try to be sensitive to feelings and attitudes so that they can act affirmatively in cases of potential dissatisfaction, suspicious behavior or unusual attitudes, work habits and life style.
J. One individual should never be totally responsible for a given activity especially if it relates to the processing or development of sensitive applications.

K. The employee morale should be kept high, to accomplish this, programs such as: fringe benefits, educational and professional development, stock options, adequate work spaces, parking areas and suggestion boxes, should be considered.

L. A special screening procedure should be available to check personal and employment records of: consultants, part-time and temporary employees, maintenance, service and janitorial personnel.

The Personnel Section Questionnaire

This section of the questionnaire is directed to collecting information about personnel policies and procedures, pre- and post-employment investigation, general management involvement in the design and revisions of security systems, and a definition of the most likely confidentiality/security threats to the organization as seen in Figure 4.

Analysis of the Results

From the results obtained in this study, it can be easily seen that large organizations use a high percentage of protective and control measures in the personnel area. A bit more of management involvement in security matters and publication of emergency plans is desired to have better coordination.
Small companies could augment their security measures in this area without increasing their expenditures very much.

If an organization cannot afford a full-time security officer or if it is not economical then a systems analyst(s) or a staff member(s) related to data processing can be appointed security officer(s) and safety committee as part of his/their responsibilities.

Once an assignment is made and somebody has been appointed responsible for the development and implementation of security measures then a security program can be started.

Managers, supervisors and employees within the firm can be asked for suggestions about protective, preventive and detection measures. This is one way to collect information and get the employees and principally management involved with security matters.

Inexpensive measures that will increase control and protection can be implemented in both small and large companies, although the study results show that only a relatively low percentage of small companies are using them. Some of the measures that can be taken are: posting and publication of emergency plans, issuing of employee identification cards, orientation about regulations and policies, form that clearly states that any misrepresentation will cause immediate dismissal, photograph taken to become part of personnel record and dismissal interviews.
<table>
<thead>
<tr>
<th>QUESTION</th>
<th>% OF &quot;YES&quot;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>LARGE FIRMS</td>
</tr>
<tr>
<td>1. GENERAL MANAGEMENT</td>
<td>100</td>
</tr>
<tr>
<td>1.1. Is there a Security Official responsible for developing and controlling security programs?</td>
<td></td>
</tr>
<tr>
<td>1.2. Is there an active safety committee which searches out and arranges elimination of safety hazards common to most commercial and industrial environments?</td>
<td>100</td>
</tr>
<tr>
<td>1.3. Are security policies, procedures and programs formally reviewed by management? How often?</td>
<td>67</td>
</tr>
<tr>
<td>1.4. Are names and telephone numbers of key personnel to be called in case of emergency clearly posted in all critical areas?</td>
<td>100</td>
</tr>
<tr>
<td>1.5. Are published copies and revisions of emergency and disaster plans distributed to all management personnel responsible for the execution of security and recovery actions in case of a disaster?</td>
<td>67</td>
</tr>
<tr>
<td>1.6. What are the most likely sources of threat to the confidentiality/security of the system?</td>
<td></td>
</tr>
<tr>
<td>1.6.1. i) Industrial espionage?</td>
<td>33</td>
</tr>
<tr>
<td>1.6.2. ii) Malicious damage or theft of information?</td>
<td>33</td>
</tr>
<tr>
<td>1.6.3. iii) Accidental invasion of privacy?</td>
<td>33</td>
</tr>
<tr>
<td>1.6.4. iv) Fraud or embezzlement?</td>
<td>67</td>
</tr>
<tr>
<td>1.6.5. v) Hardware or program failures?</td>
<td>67</td>
</tr>
<tr>
<td>1.6.6. vi) Accidental damages?</td>
<td>33</td>
</tr>
<tr>
<td>QUESTION</td>
<td>% OF &quot;YES&quot;</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>LARGE FIRMS</td>
</tr>
<tr>
<td>2. EXIT POLICIES</td>
<td></td>
</tr>
<tr>
<td>2.1. Are interviews conducted upon dismissal of employee in order to recover identification cards, keys, records and manuals, collect and observe any hostile reactions? When is employee informed of termination?</td>
<td>100</td>
</tr>
<tr>
<td>3. EMPLOYEE IDENTIFICATION</td>
<td></td>
</tr>
<tr>
<td>3.1. Is photograph of job applicant taken immediately upon employment to become part of personnel record?</td>
<td>100</td>
</tr>
<tr>
<td>3.2. Are employee identification cards issued and if so, do they include: recent photograph, signature, issuing date, means of preventing alteration?</td>
<td>67</td>
</tr>
<tr>
<td>4. VENDOR HIRING POLICIES</td>
<td></td>
</tr>
<tr>
<td>4.1. Are there adequate security procedures for:</td>
<td></td>
</tr>
<tr>
<td>4.1.1. i) Maintenance employees?</td>
<td>100</td>
</tr>
<tr>
<td>4.1.2. ii) Janitorial personnel?</td>
<td>100</td>
</tr>
<tr>
<td>4.1.3. iii) Temporary employees and consultants?</td>
<td>100</td>
</tr>
<tr>
<td>5. HIRING POLICIES</td>
<td></td>
</tr>
<tr>
<td>5.1. Does employment application form clearly indicate that any misrepresentation, falsification or withholding of information will cause for dismissal at any time after employment?</td>
<td>100</td>
</tr>
<tr>
<td>5.2. Are the applicant's personal and employment references checked by means of personal meetings, telephone or mail?</td>
<td>100</td>
</tr>
<tr>
<td>5.3. Does pre-employment investigation include a criminal records check?</td>
<td>33</td>
</tr>
<tr>
<td>5.4. Are new employees given through briefings (orientation) on the policies, regulations, and practices of the organ.</td>
<td>100</td>
</tr>
</tbody>
</table>
Physical Section

Statement of The Problem

In order to properly discuss the threats with which the physical security measures deal, it is necessary to classify them into four categories:

- Natural disasters
- Manmade disasters
- Unauthorized access
- Hardware and utility failures

Each one of these categories will be further subdivided into specific areas. It is important however, to understand that many of the problem areas are interrelated to each other, and that improvement of security in one type of threat may result in improvement of other problem areas. As can be seen in Figure 7, the threats and remedial measures are interdependent.

Physical security should be of concern not only for critical areas such as the data processing room and volume library, but for every aspect of system development and operation.
<table>
<thead>
<tr>
<th>COUNTER-MEASURES</th>
<th>National catastrophe</th>
<th>Sabotage</th>
<th>Data theft, copying, browsing</th>
<th>Snooping</th>
<th>Accidental Revelation or destruction</th>
<th>Remote terminal assault</th>
<th>Electromagnetic eavesdropping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical barriers</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guards, badges</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passwords, fingerprints</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice, signature, etc.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encrypting of data</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EM filters, shields</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auditing, checks and balances</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat monitoring</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality software, data protection, bounds control</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personnel screening, Motivation</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Terminal access controls</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File access controls</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data copies in safe storage</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Backup support equipment</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fig. 7. Threats and Countermeasures

Natural Disasters

Definition of The Threat

Natural disasters or Acts of God are a type of threat in which human intervention is non existent. The security planner has no control over the occurrence of these threats and the best measures will be the ones that will minimize the damage caused if a disaster should happen. Some of the threats that can be classified under natural disasters are:

1. Windstorm
2. Hurricane
3. Tornado
4. Earthquake
5. Fire
6. Explosion
7. Flood
8. Lightning
9. Ice and Snow
10. Rain and Mud

All of these events tend to have the same basic effects on data processing applications: complete or partial destruction of the facility and its contents and therefore, interruption of normal operations. They also represent a threat to the health and lives of the personnel. Security and protection in this field can be obtained by maintaining access controls; fire alarm, prevention and extinguishing systems; general safety and surveillance activities.

General Guidelines

Some general protective measures can be taken to minimize damage in the event of disaster:

A. An analysis of frequencies and damages caused by windstorms,
hurricanes and tornadoes in the region where the computer center is located. Information can be obtained from the local National Weather Service Office and the National Oceanic and Atmospheric Administration.

B. A study and plan should be implemented to protect the facilities against structural damage, flooding and loss of electric power due to high winds, earthquake or explosion.

C. The selection of the building: structural resistance and its location is of prime importance.

D. Emergency procedures should be available in case of interruption of transportation, supporting utilities and other vital services.

E. The security planner and systems analyst(s) should be aware of power characteristics: quality and reliability.

F. There should be measures to insure prompt detection of fire (heat and smoke detectors), adequate means and personnel to limit damage and assure prompt recovery. Some of the most common extinguishing mechanisms are:

1) Portable or hand extinguishers
2) Hose lines
3) Automatic sprinkler systems (water)
4) Volume extinguishment systems (HALON - 1301, Carbon dioxide - CO₂)

G. Combustible materials should be kept in safe places where they cannot be easily ignited and there is not likely to be a source
of ignition.

H. The building and the equipment in it can be better protected if the design and construction of the building is safe: the structure of the building is constructed of non-combustible materials; there are low-flame-spread materials for floors, walls and furniture; fire walls; stairwells, dampers or shutters in ducts.

I. Safety programs should be regularly offered to employees.

J. Documentation, cards, magnetic tapes and disks should be kept in water and fireproof vaults when not being used.

K. It is prudent to consider some countermeasures if the flooding exposure is highly probable: emergency pumps, drains, sandbags and masonry curbs.

L. An analysis of electric power line fluctuations and the effect of these in the hardware is necessary. Some fluctuations caused by lightning may generate logic errors, erroneous data transfer and even damage the hardware.

Man Made Disasters and Unauthorized Access

Definition of the Threats

Man made disasters are those in which human beings are responsible for the occurrence of a catastrophe.

The problem of unauthorized access can be discussed together with man made disasters because many of the preventive measures are common to both threats.

Most of the plans designed to minimize damage and recovery in the event of a natural disaster are also applied against man
made disasters. It is important to recognize that human beings are behind the occurrence of a catastrophe in these types of threats.

It is to be expected that intruders will find a way to penetrate the protected areas if enough time and resources are available to them and the rewards are of sufficient magnitude to make such access attractive. Thus, one thing to keep in mind at the time of designing the security measures is that the cost of obtaining some information or causing damage to the data processing system should be more expensive than the value of the information obtained or the damage caused.

General Guidelines

Protection measures against man made disasters are:

A. The best possible site for a computer complex would be an isolated one. The more remote a site is and the less cover available, the easier it is to control the access. Flat, wideopen, unpopulated spaces make identification of authorized or unauthorized persons simple.

B. The air conditioning system should be entirely self-contained and not linked to any other area; there should be no external access to ventilation systems or insurgents may be able to introduce various noxious or toxic gases.

C. There should be only one door for regular access to the data processing center. Any other doors for fire escape purposes should be kept locked from inside, it should not be possible to
open them from the outside; internal keys should be kept behind break-glass panels. It may be possible to use push-bar escape doors.

D. A perimeter barrier (wall or fence), guards and patrols, electronic burglar detectors, secure windows, strong locked doors, reinforced roofs, burglar-proof safes and store rooms, and others are possible protective mechanisms that the security planner must consider.

E. There are many electronic innovations available to protect the computer center against intruders, some of these are: light beam (or laser, ultraviolet or infrared radiation), magnet detectors, ultrasonic and radar detectors, closed-circuit television, theft detectors, magnetic strip and card readers, time-lapse cameras and electronic combination locks.

F. When evaluating the potential threats, it is necessary to estimate the likely level of effort the intruder might be willing to exert to achieve his goal. Some of the threats may come from: common criminals, activists, espionage agents, vandals, riot, strikes, sabotage and mischief.

G. The following areas constitute a minimum set to be analyzed to determine permissible access, both during operational periods and when the facility is closed: computer room, data storage library, input/output area, data conversion area, programmer areas, document library, communications equipment area, computer maintenance room, mechanical equipment room, telephone
closet and supplies storage.

H. The security planner should consider the human resources available to support the physical protection plan. In addition to full-time guards, the following people may, as permitted by regular duties, be able to participate: receptionists and information desk personnel, building and grounds maintenance staff, shipping and receiving clerks, messengers, area supervisors and mail room personnel.

I. Access controls cannot be too stringent because this could inhibit the smooth operation of the shop, frustrate loyal employees and cause bright employees to seek some way to circumvent the system. A lax set of controls tends to indirectly authorize employees access to data which may satisfy their curiosity, but it is not part of their jobs.

J. Precious files should be identified with specially colored labels and they will be kept under more rigorous control than the regular files.

Hardware and Utility Failures

Statement of The Problem

The typical computer system is composed of many interconnected units which perform the functions necessary to perform its assigned data processing tasks.

The computer, its various peripherals and the electric power necessary to keep these units running will fail occasionally. The
failure of any element would halt operations if specific measures are not taken. The reliability that has been engineered into the system will determine how often failures will occur.

General Guidelines

To maintain a basic understanding of utilities and hardware failures, the following actions are necessary:

A. The designer of the accuracy and security procedures must consider all the possible categories of failure and decide the proper course of action if each occurs.

B. It is not desirable to start a long-run again if a computer failure occurs. Therefore, the run is divided into short segments and at the end of each segment a check-point is taken, meaning that enough data has been recorded to restart the run at that point.

C. The typical automatic data processing procurement will include standards of performance demonstration required for the acceptance of a system.

D. An analysis of the loss potential based on estimates of failure rates and repair times, will permit the automatic data processing security planner to identify those hardware units where failures will be most critical to operations. Additionally, it will serve as the basis for cost justification of remedial measures, a guide for development of a contingency plan and as an aid in future procurement decisions.

E. The automatic data processing (ADP) security planner
should be aware of the following alternatives:

. Incorporate one or more additional units of a given type beyond the minimum required to have a stand-by type of situation.
. Use a substitute technique or alternate procedure.
. Install two or more computers which as a group can handle the normal work load. If one computer fails, only the least critical tasks will be interrupted.
. Install several identically configured computers so that either system can perform all assigned tasks. This approach may be used only for extremely critical or high risk missions.

F. Establish adequate policy and procedures for management of hardware maintenance. Effective maintenance management should include:

. Determine the optimum schedule and scope of preventive maintenance.
. Report and perform statistical analysis on hardware failures so as to detect significant failure trends and take remedial measures on a timely basis.
Remedial maintenance should also receive continuing attention. Efforts to reduce the mean time of repair should be cost effective.

G. There must be procedures to handle operations when the failure of the computer system is partial. The system may be able to give a degraded form of service; when a component goes out, an alternative means of processing should be available.

Some important terms for the systems planner are the following:

- **Fallback**: The system modifies its mode of operation to circumvent the error.
- **Fail softly**: The system uses alternative means of processing rather than collapsing completely in the event that a component goes out.
- **Bypass procedure**: Standby procedure that enables the regular continuation of critical operations without assistance from the computer.

H. System controls should not allow errors or security violations during the periods of difficulty when failures are encountered.

I. Computer and terminal operators must be carefully trained in what to do when failures occur. They must be able to initiate the fallback and recovery action.
J. The ADP security planner should consider the probability of occurrence and the consequences in the event of failure of the following supporting utilities: electric power, air conditioning, communications, water, elevators and general supplies.

Description of The Physical Area Questionnaire

This section includes facility access controls for visitors and employees, guarding and surveillance activities, fire prevention, alarm systems, maintenance and safety, as seen in Table 5.
# TABLE 5

**PHYSICAL SECTION COMPARISON OF RESPONSES**

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>LARGE FIRMS</th>
<th>SMALL FIRMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <strong>ACCESS CONTROLS</strong></td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>B.1.1. If badges do not have means to prevent alteration, are employee badges issued and returned as employees enter or leave, and are all other badges kept on the premises always accounted for?</td>
<td>67</td>
<td>60</td>
</tr>
<tr>
<td>B.1.2. Are there access control procedures defined to handle visitors, maintenance, service and other personnel?</td>
<td>100</td>
<td>40</td>
</tr>
<tr>
<td>2. <strong>PROTECTION EQUIPMENT</strong></td>
<td>100</td>
<td>40</td>
</tr>
<tr>
<td>B.2.1. Is surveillance and fire extinguishing equipment checked regularly?</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>B.2.2. Are there readily accessible portable (or hand-hose system) fire extinguishers in and around the computer facility?</td>
<td>100</td>
<td>60</td>
</tr>
<tr>
<td>B.2.3. Is there an alarm system with smoke censors and automatic fire extinguishing equipment (such as water sprinklers, carbon dioxide, high-expansion foam, or Halon) located in the computer facility and data library or area where magnetic tapes, disks, and other records are stored?</td>
<td>100</td>
<td>40</td>
</tr>
<tr>
<td>3. <strong>HOUSEKEEPING</strong></td>
<td>100</td>
<td>40</td>
</tr>
<tr>
<td>B.3.1. Are all accumulations of flammable material in or around the data processing site removed to avoid a potential fire hazard?</td>
<td>60</td>
<td></td>
</tr>
</tbody>
</table>
Analysis of The Results

Large organizations are applying most of the basic protection measures investigated by the questionnaire. The access control procedures can be improved in some companies if the data processing and library centers are relocated to a building (or floor of a building) exclusively for their use and coded locks used (magnetic strips).

Small firms can very inexpensively improve methods of protection in this area. As discussed earlier in the Personnel Section, badges are not very costly; access control procedures can be implemented without going to very sophisticated and expensive equipment, by using locks (combination, magnetic or regular) in the doors which lead to the computer center and data library. The fire extinguishing equipment (automatic or manual) should be checked regularly (following manufacturer's specifications) to assure proper functioning in the event of an emergency. Some means of directing early fires are necessary to avoid the spreading of flames, for this there are smoke and heat sensors available at reasonable prices.

The removal of flammable materials from the data processing and library centers is important in order to avoid a potential fire hazard. Carbon copies and liquid cleaners can be kept in fire-proof storage areas (special plastic or steel cabinets).
Data, Programs and Documentation Section

Statement of The Problem

Computer applications can be manipulated by altering the input data or the software.

Software are sets of instructions which are stored in the computer memory bank or in off-line storage devices (magnetic tapes, disks, cards and cassettes). There are two major types of software used in computer systems: operating system software and user or application software.

The operating system is a set of programs (generally provided by the hardware manufacturer) which provides "services" to the computer user. The services rendered by the operating system software vary with the size of the computer system. Usually, most of these services provided are: schedule an application program, load scheduled program(s), allocate core, disk and devices to that program, handle all the Input/Output and interrupts. Security requirements for operating system will not be discussed in this report.

The user software is designed to make the computer accomplish a specific application. This type of software can be developed in-house or bought from a commercial software firm.

Manipulation of user programs is divided into two classes: first, the program itself can be altered; second, the input data to the program can be altered or both.
Documentation is the means by which a current status of the system is described; instructions on how to operate the system, recovery procedures in case of failure, testing and security measures should be included as part of the documentation.

An acceptable level of security in this area can be obtained by the use of highly detailed and accurate procedures; operating instructions and documentation; programs, data and storage controls, and record handling procedures.

General Guidelines

Control and security procedures which should be included under data, programs and documentation are the following:

A. Basic controls over the accuracy of the operation may help to minimize erroneous operations and therefore, maintain a high degree of control. Some of these accuracy controls are:

- Verify data after keypunching; the verifier operator and the card punch operator should be two different persons.
- Input validation checks.
- A quality-control function to sample the accuracy of data could be established.
- Errors could be analyzed by sources, type, quantity, magnitude, age and any other factors that might help to control them and pinpoint problems.
B. Types of data validation checks that should be established are:

- Character checks (test for numeric, alphabetic, special character, blanks and sign).
- Field checks (limit test, range test, valid item, consistency, sequence check, reasonableness test).
- Transaction checks (test for completeness, serial number checks, false punching and valid item).
- Batch checks (transaction count, batch control totals, hash totals and batch number checks).

C. External controls by means of a control group. This input/output control group is the interface between the users and the computer operations.

D. Data, programs and associated documentation should be controlled to the extent that they are available only to the personnel actually involved with their use and development.

E. If the information being transmitted from one center to another is confidential and highly sensitive, cryptography can be used to prevent the unauthorized individuals from having access to the text.

F. Programs should be tested for improbable, illegal and impossible input. There should be a test criteria for all programs
depending on importance, function, complexity and sensitivity.

G. Every change in any program should be authorized, certified and documented with no exceptions.

H. Installation of a new program should occur only after thorough program and system tests have been completed and approved. No program should be accepted without adequate and complete documentation which has been reviewed and approved by a control group.

I. The chief programmer team concept, which will tend to make a program module less of an individual possession, should be considered as a possible implementation in the programming control program.

J. Better documentation procedures, structured design and structural programming will facilitate the reading of programs and therefore, increase the control over programming.

K. The security planner should consider what algorithms, mathematical processes or computer processing schedules are valuable to a competitor and protect them against any transgressor access.

L. Every program documentation package should contain: program description, system flowchart, program flowchart, current compilation or assembly listing, record layouts, sample inputs/outputs, operating instructions, job control cards, control access codes, program changes log and documentation.
M. Four principles that summarize a number of preventive measures are:

- The programming and operational work should be divided into slices handled by different groups.
- Only authorized programs may be run in the system.
- The computer-room hardware should be handled exclusively by operations personnel.
- Programmers must be fully aware that their work is being monitored and that audit trails will make it possible to pin the blame for any malfunction.

N. Standard security procedures should be established and made required of all computer personnel.

Description of The Questionnaire Regarding Data Programs and The Documentation Area

This area was designed to collect information about data library procedures and access controls; use of operating instructions and documentation; storage facilities; data handling; retention and destruction processes; also logging and control over equipment's use. Reference Table 6.
<table>
<thead>
<tr>
<th>QUESTION</th>
<th>% OF &quot;YES&quot; _LARGE FIRMS</th>
<th>% OF &quot;YES&quot; _SMALL FIRMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ACCESS AND CONTROL FOR DATA PROGRAMS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.1.1.1. Do computer generated reports have:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.1.1.2. i) A cover sheet which contains job identification, files used, date and security classification?</td>
<td>67</td>
<td>40</td>
</tr>
<tr>
<td>E.1.1.3. ii) Each page numbered sequentially?</td>
<td>67</td>
<td>60</td>
</tr>
<tr>
<td>E.1.1.3. iii) Follow the last page of output with a statement signifying end of output, security classification and number of pages printed?</td>
<td>33</td>
<td>20</td>
</tr>
<tr>
<td>E.1.2. Are there systematic procedures for the disposal of sensitive information? Are old printouts, carbon paper, tapes, ribbons, and documents exempted and shredded?</td>
<td>100</td>
<td>60</td>
</tr>
<tr>
<td>E.1.3. Are magnetic tapes, disks, documents, microfilms and other supplies kept in fire-proof and water-proof vaults and out of sight?</td>
<td>100</td>
<td>50</td>
</tr>
<tr>
<td>E.1.4. Are computer forms which might be used to perpetrate embezzlement or fraud, such as continuous form checks and official notices, imprinted with sequential numbers which are recorded to control usage of these forms?</td>
<td>100</td>
<td>60</td>
</tr>
<tr>
<td>E.1.5. Is an up-to-date list of computer applications and programs maintained in catalog form?</td>
<td>100</td>
<td>60</td>
</tr>
<tr>
<td>E.1.6. Are there controls to ensure that material from the data library are issued and delivered to authorized personnel only, and a library log maintained to ensure close control and prompt return of materials after use?</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>QUESTION</td>
<td>LARGE FIRMS</td>
<td>SMALL FIRMS</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>E.1.7. Are authorized lockwords, keys, or encoded badges to enable the</td>
<td>67</td>
<td>25</td>
</tr>
<tr>
<td>operation of time-sharing, remote job entry, and other on-line terminals?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.1.8. As part of security measures for on-line systems, are reports</td>
<td>67</td>
<td>25</td>
</tr>
<tr>
<td>regularly produced showing attempts to use invalid lock-words and illegal procedures?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.1.9. Where general purpose data base management systems are used, are</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sensitive or privileged data elements controlled by security codes which</td>
<td></td>
<td></td>
</tr>
<tr>
<td>must match the user's authorization level to enable them to be accessed?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.1.10. Are financial and asset control systems transactions placed under control at their point of origination?</td>
<td>100</td>
<td>50</td>
</tr>
<tr>
<td>2. LOGS AND INSTRUCTIONS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.2.1. Are written procedures provided to instruct the console operator</td>
<td>100</td>
<td>60</td>
</tr>
<tr>
<td>to what actions are to be taken when the system controls and counts do</td>
<td></td>
<td></td>
</tr>
<tr>
<td>not check out, unanticipated equipment difficulties, or program running</td>
<td></td>
<td></td>
</tr>
<tr>
<td>problems such as unexplained messages or halts?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.2.2. Are &quot;file protect rings&quot; for tapes removed immediately after a</td>
<td>67</td>
<td>0</td>
</tr>
<tr>
<td>tape is created and dismounted from tape drive?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.2.3. Is a rule enforced requiring that when occupied, at least two</td>
<td>33</td>
<td>0</td>
</tr>
<tr>
<td>people be present in the data processing center?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.2.4. Is checking and enforcement of security procedures during</td>
<td>100</td>
<td>40</td>
</tr>
<tr>
<td>operations designated as a specific responsibility of appropriate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>supervisory personnel?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
TABLE 6 -- Continued

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>LARGE FIRMS</th>
<th>SMALL FIRMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.2.5. Are operations on off shifts spot checked? Do the logs and audit</td>
<td>67</td>
<td>25</td>
</tr>
<tr>
<td>paperwork always reflect the actual status?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.2.6. Are data received or issued by the data processing department</td>
<td>33</td>
<td>20</td>
</tr>
<tr>
<td>logged in by batch showing date, time, name of data, quantity, from</td>
<td></td>
<td></td>
</tr>
<tr>
<td>whom data were received and to whom it was issued?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.2.7. Does the console written log sheet run identification, setup</td>
<td>67</td>
<td>20</td>
</tr>
<tr>
<td>time, processing start/stop time, malfunctions and down time? Are</td>
<td></td>
<td></td>
</tr>
<tr>
<td>these logs carefully checked by operations supervisors for complete-</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ness and accuracy, and analyzed for recurrent problems and anomalies?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E.2.8. Are data processing equipment central processing unit (CPU)</td>
<td>100</td>
<td>60</td>
</tr>
<tr>
<td>meters regularly read, logged, and reviewed for possible unauthorized</td>
<td></td>
<td></td>
</tr>
<tr>
<td>use of equipment?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

51% OF 11 YES
Analysis of The Results

Both large and small companies should increase the usage of cover sheets (containing job identification, security classification, date, files used), sequentially numbered pages and a last page (signifying end of output, total number of pages, and security classification) in order to improve controls over theft of information.

To obtain information from the system or change existing data, it is necessary to have access to the system. If access to the system is to be limited to authorized personnel only, then authorized lockwords, keys or encoded badges should be used to enable the operation of time-sharing, remote job entry terminals.

It is important to have reports that show attempts to use invalid keywords and illegal procedures, this information will alert the security officer of possible threats and the code or keyword designer with a measure of the user's difficulty in using the passwords or codes.

It should be a policy that at least two people be in the computer center when this is in operation. If an accident occurs one person can help the other and moreover, it is harder to alter data or steal information if someone else is present.

The data received and issued by the data processing department should be logged in by showing date, name, quantity, from whom data was received and to whom it was issued. This procedure will augment the degree of control. The unauthorized use of equipment can be
detected and controlled by checking regularly the CPU meters and reviewing the console written log.

**Backup Section**

**Statement of The Problem**

A failure in hardware, software or personnel is to be expected. Failures and errors are inevitable in the operation of any computer system, therefore, the security planner, systems analysts and management should plan on how to handle the computer operations when failure occurs.

Most companies cannot afford operational shutdowns; the business may come to a halt, moreover the computer downtime can be very expensive and may cause costly delays in accomplishing some critical functions.

Backup operations may take place on-site when there is only a partial loss of capability but may require one or more off-site locations when there has been major damage or destruction.

The emergency procedures necessary when a failure occurs vary with the type of equipment and its use in the operation. Nevertheless, some general procedures can be stated. Security in this area may be obtained by the careful planning and coordination of backup facilities, interruptions and failure recovery procedures.

**General Guidelines**

Backup resources should be available when needed. Some general principles to provide backup facilities are:
A. An effective planning approach should include an appraisal of each individual piece of equipment and the effects of its failure in the overall processing system; followed by laying out a plan for an alternate method of processing.

B. An equipment feasibility study should balance the need for backup equipment with the requirements of financial reality.

C. Backup equipment should not be located in the same site because the same disaster can cripple both the principal and backup equipment.

D. It is important that approved security procedures continue in force, even if the data processing center is functioning under emergency operations.

E. It may be advisable to explore having available electrical power backup, temporary power source, an independent air conditioning backup and trained personnel backup.

F. Assurance that compatible backup facilities will be available during a crisis is a very critical point. Identical hardware is not sufficient to assume that both systems configurations are the same.

G. A written agreement should be signed by officials of both companies that are involved in an agreement to exchange backup facilities.

H. If a satisfactory backup contract cannot be worked out with a computer service bureau or a nearby compatible data
processing center, then it may be necessary to go to the additional expense to maintain redundant systems.

I. Data preparation facilities, proper forms and other data media should be considered in the overall backup plan.

J. Some basic guidelines to stretch the backup facilities are:

- Postpone less urgent tasks.
- Substitute other procedures.
- Modify tasks to reduce run time.

K. Each backup plan should cover these five basic areas:

- Performance specifications (performance of each task will depart from normal).
- User instructions (emergency procedures, what to do).
- Technical requirements for each data processing task (documentation of operational requirements for each task).
- Computer system specifications (terms and cost of backup use, location of the system, schedule of availability for backup operation, and the tentative schedule of ADP tasks to be performed on the system).
- Administrative information (special personnel assignments and procedures, temporary employment, use of special messengers and other departures from normal).
A recovery planning program should be started once the damages have been calculated and basic requirements have been defined (floor space to house the ADP facility, ADP hardware, supplies and utilities).

The security planner may propose some types of insurance coverage and management will decide what to do. Some types of insurance coverage are: equipment and facilities; storage media and its contents; loss due to business interruption; extra expense at a backup site; valuable papers and records; malpractice, including human errors and omissions.

Description of The Questionnaire Concerning The Backup Area

Equipment backup and fallback, contingency plans, agreements with the backup site and protection of support facilities are considered in this section as in Table 7.
# TABLE 7

## BACKUP SECTION COMPARISON OF RESPONSES

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>LARGE FIRMS</th>
<th>SMALL FIRMS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. BACKUP AND FALBACK</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1. Have contingency plans and priorities been developed and tested out for the handling of computer shutdowns for a period of:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1.1. i) 1-3 days</td>
<td>33</td>
<td>20</td>
</tr>
<tr>
<td>1.1.2. ii) 1 week</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1.1.3. iii) 2 weeks</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1.1.4. iv) more than two weeks</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1.2. Is backup computer equipment configuration checked often for changes and alterations that could affect compatibility for backup purposes?</td>
<td>67</td>
<td>40</td>
</tr>
<tr>
<td>1.3. Is it realistic to expect that appropriate data processing equipment can be made available at time of need in quantity sufficient to enable near normal functioning?</td>
<td>67</td>
<td>40</td>
</tr>
<tr>
<td>1.4. Are there adequate physical damage protections for support facilities external to the building such as: air conditioning, telephone, electric power and water?</td>
<td>100</td>
<td>20</td>
</tr>
<tr>
<td>1.5. Have procedures for operating at the backup site been documented?</td>
<td>67</td>
<td>0</td>
</tr>
<tr>
<td>1.6. Does the agreement with the backup site cover:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.6.1. i) Physical access by your operations people?</td>
<td>67</td>
<td>20</td>
</tr>
<tr>
<td>1.6.2. ii) Priorities, in the event you are dynamically sharing their equipment?</td>
<td>67</td>
<td>20</td>
</tr>
<tr>
<td>1.6.3. iii) Charges for services received?</td>
<td>33</td>
<td>0</td>
</tr>
<tr>
<td>1.6.4. iv) Assignable locked storage for holding your classified materials?</td>
<td>33</td>
<td>0</td>
</tr>
<tr>
<td>QUESTION</td>
<td>% OF &quot;YES&quot;</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>v) Use of telephones &amp; office areas?</td>
<td>33</td>
<td>20</td>
</tr>
<tr>
<td>Are the costs of maintaining portability of applications and compatibility of computer systems included in your regular budget?</td>
<td>100</td>
<td>20</td>
</tr>
</tbody>
</table>
Analysis of The Results

It can be noticed from the results obtained that contingency plans have not been developed and properly tested out. Both large and small organizations must improve in this area in order to avoid a complete halt of operations for several days.

It is not sufficient to expect that compatible backup equipment will be available when needed. More than just one facility should be available. Also, a signed contract should exist specifying the cost for services, the amount of time available, storage, telephone and office areas, access and any other special procedures.

The protection for support facilities will change from zone to zone. The Orlando area is within a critical zone of tornadoes and thunderstorms.

It is important to analyze how these events will affect the performance of the equipment and how much backup or protective measures are required.

Program Development Section

Statement of The Problem

The data processing security planner and his staff can identify a set of remedial measures which appear to be the most effective against all threats, but all they can do is recommend this group of remedial measures. It is up to management to approve what actions should be taken.
Two phases of security are: the responsibility for the design of security techniques and procedures, and the responsibility for the day-to-day operations given that design. In both areas the overall responsibility lies with management.

Data processing management (and the security staff) should be aware that it is their duty to maintain top management informed of the organization's vulnerability if a disaster should strike its computer system.

Top management should see that an overall strategy for security is established and that the security procedures are strictly enforced.

General Guidelines

Some procedures and management actions are necessary to maintain a sound security program, such as:

A. Information such as that which follows should be made available to management:

. Significant threats and probabilities of occurrence.
. Critical tasks and the loss of potential related to each threat.
. A list of remedial measures which will yield the greatest net reduction in losses, together with their annual cost.
B. The responsibilities for secure design should be divided. One possible way is:

- Overall coordination
- Technical design
- Procedural controls
- Controls on programs and programmers
- Physical security
- External administrative controls
- Auditors

C. The responsibilities for maintaining security of day-to-day operations may be divided as follows:

- Data-processing manager
- Security administrator
- Local security officers
- File owners
- Line managers
- Auditors
- All staff

D. Management should enforce security procedures that will ensure the integrity and accuracy of the data required to plan and control the enterprise, provide for the privacy of proprietary, personal, privileged or otherwise sensitive data, and protect and conserve the organization's assets from natural disasters, man made hazards, vandalisms and theft.
E. The strategy for security should be a sound, continuing one, not, as has often been the case, one based on passing fashion or reactions to emergencies.

Description of The Questionnaire Related To The Program Development Area

This section deals with the design and implementation of computer programs and control procedures. It also includes a set of questions about the documentation included in each program and regulations such as: audit trails, information loss, error detection and balances. This information is detailed in Table 8.
TABLE 8
PROGRAM DEVELOPMENT SECTION
COMPARISON OF RESPONSES

<table>
<thead>
<tr>
<th>QUESTION</th>
<th>LARGE FIRMS</th>
<th>SMALL FIRMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. PROGRAM DEVELOPMENT PROCEDURES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1. Are systems audit and control procedures for new systems designs put through a formal approval process by the internal audit department?</td>
<td>100</td>
<td>33</td>
</tr>
<tr>
<td>1.2. With regard to programming, are logic reviews conducted with a programming manager or another programmer to minimize the probability of undetected logic errors that could crop up during live systems operations?</td>
<td>100</td>
<td>50</td>
</tr>
<tr>
<td>1.3. Are there established standards that specify the internal construction and programming techniques to be used for secure application programs?</td>
<td>67</td>
<td>20</td>
</tr>
<tr>
<td>1.4. Is program certification performed under the surveillance of an internal auditing or quality assurance group administratively separate from the programmers who performed the coding?</td>
<td>67</td>
<td>0</td>
</tr>
<tr>
<td>1.5. Does the documentation package include for each program:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.5.1. i) Program description?</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>ii) System flowchart?</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>iii) Current compilation or assembly listing?</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>iv) Record layouts?</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>v) Sample input/output?</td>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>vi) Operating instructions?</td>
<td>100</td>
<td>67</td>
</tr>
<tr>
<td>vii) Job control cards?</td>
<td>67</td>
<td>100</td>
</tr>
<tr>
<td>viii) Program changes (date, description, approval)</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>ix) Control access codes?</td>
<td>67</td>
<td>0</td>
</tr>
<tr>
<td>x) Duplicate documentation stored off-premises?</td>
<td>33</td>
<td>33</td>
</tr>
<tr>
<td>QUESTION</td>
<td>% OF &quot;YES&quot;</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>LARGE FIRMS</td>
<td>SMALL FIRMS</td>
</tr>
<tr>
<td>1.6. Are one or more individuals on the internal audit staff capable of interpreting program coding and writing basic programs?</td>
<td>100</td>
<td>25</td>
</tr>
<tr>
<td>Are there appropriate techniques for:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.7.1. i) Proper sequencing?</td>
<td>100</td>
<td>40</td>
</tr>
<tr>
<td>1.7.2. ii) Batch totals?</td>
<td>100</td>
<td>80</td>
</tr>
<tr>
<td>1.7.3. iii) Record counts?</td>
<td>100</td>
<td>40</td>
</tr>
<tr>
<td>1.7.4. iv) Transaction completeness?</td>
<td>33</td>
<td>40</td>
</tr>
<tr>
<td>1.7.5. v) Tests for minimum and maximum values?</td>
<td>33</td>
<td>20</td>
</tr>
<tr>
<td>1.7.6. vi) Error-checking and control routines for input validity?</td>
<td>100</td>
<td>40</td>
</tr>
<tr>
<td>1.7.7. vii) Exception reporting where arithmetic data on file exceeds predetermined customary range?</td>
<td>67</td>
<td>20</td>
</tr>
</tbody>
</table>
Analysis of The Results

It is vital to maintain control over the computer programs in order to prevent fraud or embezzlement. The results show that small companies do not exercise enough regulation over the internal construction of computer programs and the certification of these by an internal audit or a quality assurance group.

Both, large and small companies should increase their control over computer programs. Most of the incidents (stealing of money or other assets) have occurred because of the lack of appropriate controls.

Improvement in the areas of predefined customer ranges and exception reporting system is necessary to detect drastic changes from the customary actions.

System and operational documentation is necessary for recovery in case of a disaster.

The results show low usage of off-premises storage of documentation.

Record counts and transaction completeness are important factors in the accuracy of the system; this is another area that should become better controlled.
CHAPTER V

CONCLUSIONS

As is stated in International Business Machines Corporation, Data Processing Division 1974, p.1:

With the greater use of computers, security has taken on new importance, a different dimension. More of your working information is stored in the system. You are more dependent on this single source for collected information. And this concentration of assets in one spot increases their vulnerability. So it is to your advantage to know how to protect your computer and its environment.

It is very important to understand the role that security plays in computer systems in order to dedicate the necessary resources to the development of efficient protective measures.

It is unfortunate that ("Computer Security...the Imperative Nuisance", 1974, p.24):

To many executives, security means an elderly, gray-haired guard sleeping out his semi-retirement at a factory door, silver tape around the windows and a fire extinguisher hanging in the hall. Nobody likes to think about security. No one wants to believe it's really needed.

These two ideas summarize the concepts that were desired to discuss in the process of writing this report.

Automatic data processing security, privacy and confidentiality problems have introduced serious stresses to management and the computer practitioner. It is the responsibility of these people to ensure that a firm's privacy and assets are protected against malefactors. Instead of finding that some minimum standards of security have been required in all firms, it has been
found that the remedial measures differ markedly in their popularity of use.

If more proficient security systems are to be used, it is necessary to define some basic areas that need to be controlled and design basic protective, preventive and detection measures.

In this study, five areas have been presented (personnel, physical, backup, development, data, programs and documentation) and the design and implementation of general countermeasures defined.

Basic concepts were defined and can be summarized as follows:

Privacy is a property of individuals. Confidentiality is a property of data. Security is a property possessed by hardware and software systems and facilities. (Davis 1974, p.23).

As has been discussed, there is not a set of solutions that will solve everybody's security problems. A procedure however, has been suggested for developing and implementing a security program. These steps are:

1. Analyze risk as the basis for development of a security policy (audit and appraise the potential security exposure).
2. Select and implement appropriate security measures to reduce exposure to losses.
3. Develop contingency plans for back-up operation, disaster recovery and emergencies.
. Provide indoctrination and training for personnel.
. Plan and conduct continuing tests and audits and adjust security measures and contingency plans as needed.

It must be emphasized that the effective use and design of security procedures will depend upon steps taken by management.

All concerned must be convinced of management's determination to see that the security measures are conscientiously executed and appropriately followed up.
APPENDIX
Fig. 8. Summary of Results, Personnel Section Large Organizations
Fig. 9. Summary of Results, Personnel Section
Small Organizations
Fig. 10. Summary of Results, Physical Section Large Organizations
Fig. 11. Summary of Results, Physical Section Small Organizations
Fig. 12. Summary of Results, Data, Programs and Documentation Section
Large Organizations
Fig. 13. Summary of Results, Data, Programs and Documentation Section
Small Organizations
Fig. 14. Summary of Results, Backup Section
Large Organizations
Fig. 15. Summary of Results, Backup Section
Small Organizations
Fig. 16. Summary of Results, Development Section
Large Organizations
Fig. 17. Summary of Results, Development Section
Small Organizations


