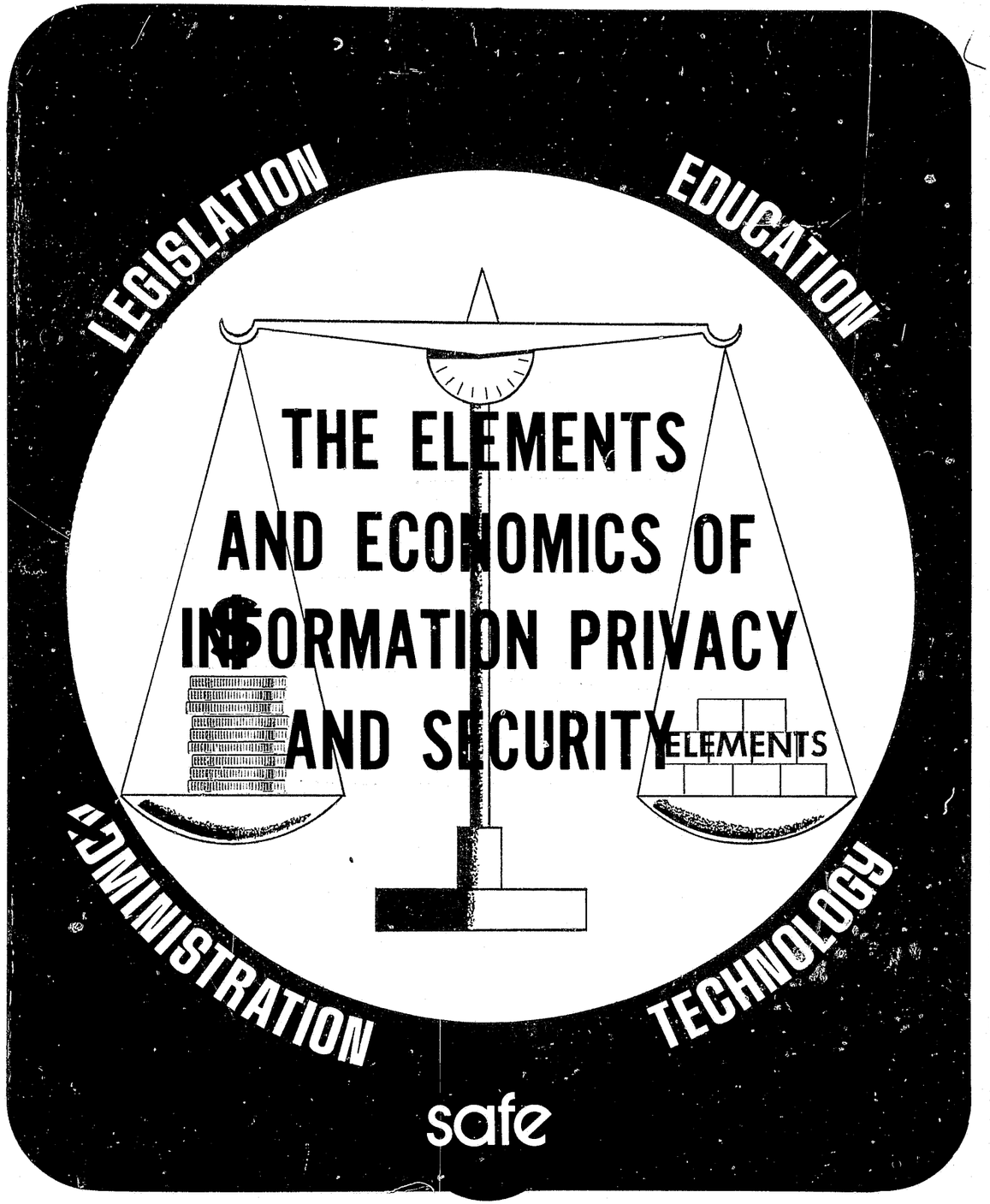


— PROJECT SAFE —

THE SECURE AUTOMATED FACILITY ENVIRONMENT PROJECT

Robert T. Caravella	Project Manager
Kenneth C. Durbin	Technology Coordinator
A. Scott Hamel	Chief Technical Consultant, Systems Engineer IBM Corporation
Linda R. Hirshman	Education Coordinator, Attorney at Law Jacobs, Gore, Burns & Sugarman
Robert T. Shoup	Software Security Officer
Gregory L. Smith	RSS Installation Coordinator
Donald E. Tolva	Legal Counsel, Attorney at Law Martin, Craig, Chester & Sonnenschein
Karen S. Collebrusco	Project Secretary

ADVISORY GROUP

John L. Gentile	Project Director Assistant Postmaster General, Management Information Systems U.S. Postal Service
Ronald W. Brady	Vice President, University of Illinois
Ted E. Climis	Vice President, System Development Division IBM Corporation
Robert R. J. Gallati	Vice President, Delehanty Institute
Arthur R. Miller	Professor of Law, Harvard Law School

In addition, the Project would like to acknowledge the outstanding contributions made by:

Robert L. Haughey, Executive Director, and the Management and Staff of the Management Information Division, State of Illinois

A. T. Kearney, Inc. Management Consultants, Chicago, Illinois

The Wordshop, Inc., Noblesville, Indiana

Harvey A. Bleam	Site Coordinator, IBM Corporation
Dr. Robert E. Bohrer	Associate Professor of Mathematics, University of Illinois
Thomas W. Boxell	Project Field Engineer, IBM Corporation
Ross W. Lathrop	Research Associate, University of Chicago Industrial Relations Center
Alan B. Griest	Manager, RSS Maintenance IBM Corporation
Dr. James H Opelka	Assistant Professor of Mathematical Systems, Sangamon State University
Dr. Charles Pinkus	Associate Professor of Quantitative Science, Sangamon State University

Finally, the Project wishes to recognize all individuals within the agencies subject to the Governor and the Office of the Secretary of State who contributed their time and ideas to the Project. A special thanks belongs to the Department of Public Health, Mental Health, Vocational Rehabilitation, the management of the Department of Finance and the IBM Springfield Branch for their particularly substantive contributions to the Project.

FOREWORD

As Information Systems Executives, we have a responsibility to maintain a proper balance between our need for information and the individual's right to personal privacy. Like our developing ecology problems, data security and privacy in information systems has developed into another potential malady for our technology-oriented and efficiency-minded society.

Due to a lack of time, inadequate funding, and the absence of available tools and evaluation techniques, information system managers have responded to the problem with a few token gestures — spasmodically implementing a few technological and administrative safeguards within their budgetary constraints. This approach has been costly and has not produced adequate safeguards as evidenced by some highly publicized unauthorized incursions into information systems.

A task force of computer specialists, statisticians, operations researchers, educators, lawyers, administrators and management consultants has addressed this problem in an actual operating environment. The tools and guidelines they developed are presented in this book. By publishing these results, we hope to:

- Augment the body of knowledge related to security and privacy in information systems,
- Stimulate discussions of alternative techniques and approaches to this problem,
- Provide practical tools and guidelines for the use of the information technologist, and
- Indicate areas where additional research or development is required or desirable.

There is nothing magic or sacred about the content of this document. Indeed, many other operating environments can perform the same type of study if they are willing to commit the time and money. Hopefully, the results of Project SAFE will allow information system users, operators and designers in government and industry to have the facts without making that substantial research and development commitment. It remains for you and your staff to tailor these results into a suitable plan to be implemented within your organization.

Robert L. Haughey
Executive Director,
Management Information Division

TABLE OF CONTENTS

CHAPTER I: WHAT IS PROJECT SAFE?

INTRODUCTION

The Secure Automated Facility Environment (SAFE) Project began in October, 1972. The project fulfilled an agreement between the IBM Corporation and the State of Illinois and established the Management Information Division of the Department of Finance as a data security and information privacy study site.

The Management Information Division (MID) is empowered by statute to provide policy and master plan direction as well as computer services to the agencies subject to the Governor. MID's enabling legislation further directs the division "to provide adequate security protection" and "to ensure the privacy of electronic data processing information as provided by law."

Through the use of an automated statutory retrieval system, the MID provides the agencies it serves with excerpts of specific privacy requirements affecting their legislated programs. This information is necessary to determine which files require special protection. Improving internal security to satisfy these statutory obligations, then, was a key reason for entering into this agreement.

Equally important, however, was the State of Illinois' committment to go beyond state government's traditional role of merely regulating and providing direct services to the private sector. It was felt that state government should also provide guidelines and a sense of direction to the private sector on sensitive social issues and that there is no better way to achieve this goal than through exemplary actions.

THE OBJECTIVES OF PROJECT SAFE

The establishment of Project SAFE in the State of Illinois was predicated on two very basic assumptions:

1. **An individual's right to privacy is a fundamental value basic to the functioning of an individual in a free society and is, therefore, worth preserving.**
2. **Computers are necessary technological information processing developments that must exist and function within the administrative and legal framework of our society.**

The long range objective of government and industry, then, must be to assure that an individual's right to privacy is protected in information systems.

Project SAFE has attempted to take practical steps toward this goal by:

1. Demonstrating an acceptable degree of protection for the pilot agency data base currently maintained at MID.
2. Analyzing and documenting security measures and their attendant costs in a complex data center.
3. Assessing the general applicability of this new body of knowledge for government and industry at large.

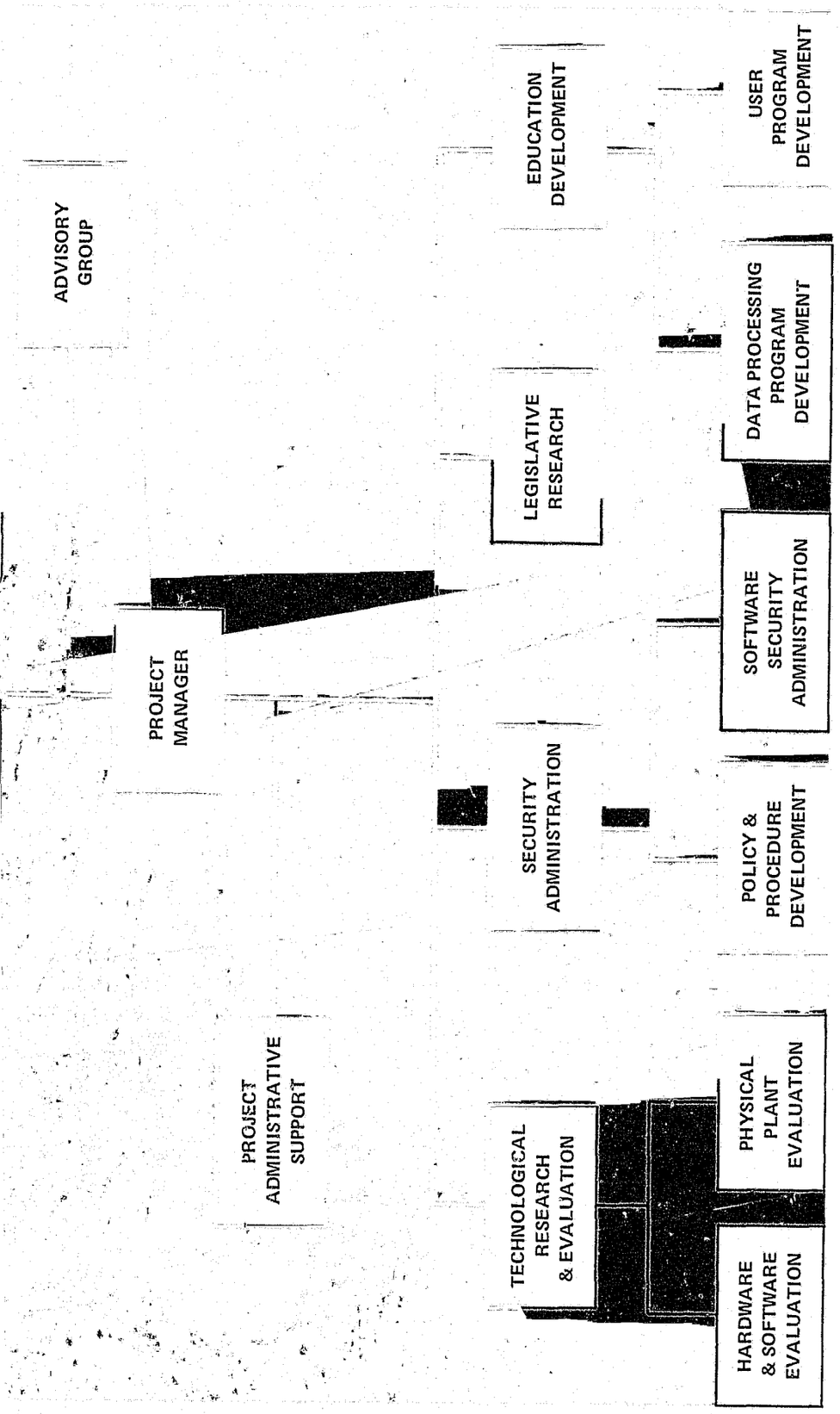
AN INTERDISCIPLINARY APPROACH

The subject of privacy and security in information systems has been approached by computer specialists, security device proponents, legislators and administrators, and each group brings concerns and prejudices peculiar to its profession and line of expertise. No one group, however, can possibly be aware of all the problems and questions that enshroud this multifaceted issue.

Project SAFE is based on a balanced interdisciplinary approach to solving the information privacy problem.

A multidisciplinary task force of lawyers, administrators, educators, management consultants, statisticians, operation researchers and computer specialists was organized. Over forty individuals within these professions have contributed to the project.

The results of the project provide executive and data processing management with realistic and practical tools and approaches to address the information privacy and data security problem. Furthermore, the report should provide a useful framework for further research and will lead to the development of future programs — programs that can expand this base of research knowledge and address areas that are beyond the purview of this project.



OPERATING ENVIRONMENT

- The Management Information Division data center has both computer operations and software support responsibility for approximately thirty Illinois state agencies. These agencies are charged back for use of data center resources based on a complex resource accounting system. Chargeback rates are influenced by the cost of hardware, software, and personnel required to support agency workloads.

- Approximately 26,000 batch jobs are processed each month at the data center. About 320 terminals comprise five independent teleprocessing systems. In addition, the data center supports 24 remote job entry stations. The use of telecommunications is expected to continue growing in light of the state's emphasis on consolidating data centers to achieve the benefits of economies of scale.

- At this writing, the MID data center consists of two 370/165s each with three megabytes of main storage sharing a pool of input-output devices, including 2 drums, 40 tape drives, and 56 3330 spindles. Of the software systems, CICS, IMS and HASP-RJE support the majority of the applications at the MID. However, the data center also supports numerous non-IBM software systems. Typically, the hardware configuration in the data center is re-evaluated and changed periodically to support the growing needs of the user community.

ORGANIZATIONAL SETTING

The Department of Finance is an agency subject to the Governor of Illinois. The Management Information Divsion is the largest division reporting to the Director of Finance. The project was established as a separate entity working in conjunction with the MID staff reporting, however, directly to the Deputy Director of the Department. All operational matters were handled through existing channels within the MID. Priority conflicts between the project and the MID were settled by the Deputy Director.

The project was organized by discipline as illustrated on the opposite page, and each discipline was responsible for the execution of the following specific functions.

- **The Legislative Research** discipline performed two independent functions:

  1. Research and analysis of existing and pending legislation in the states and the federal government,
  2. Development of model state legislation to address the privacy problem (which was not funded by IBM).

- **The Technology Research and Evaluation** discipline involved three functional areas:

  1. Installation and evaluation of a prototype software security system known as the Resource Security System (RSS).
  2. Measurement of the impact of RSS on system operating performance and reliability,
  3. Investigation and installation of physical protection devices to enhance internal physical security.

- **The Security Administration** discipline was divided into three functions:

  1. Development of security profiles for specific pilot agencies,
  2. Real time administration of the software security system,
  3. Development of appropriate policy and substantive procedures.

- **The Education Development** discipline involved the development of a program of education for the Management Information Division personnel and the Agencies subject to the Governor.

A weekly technical review meeting was held to provide organizational flexibility and to encourage the establishment of routine communication between project members and the MID staff. This meeting proved to be an invaluable vehicle for communicating the problems and activities of the MID software and operations staff to the Project Team.

INFORMATION SYSTEMS ENVIRONMENT

The MID data center processes and maintains large quantities of personal information including:

- Vital statistics (births, deaths, marriages, divorces)
- Communicable diseases
- Employee payroll records
- Mental health inpatient records
- Adoption records
- Licensing records
- Welfare recipient records

Three state agencies were asked to participate as pilot agencies — the Departments of Public Health and Mental Health and the Division of Vocational Rehabilitation. These agencies provided a representative sample of the type and size of users processing their workloads at MID.

In addition to the types of confidential information mentioned above, the MID maintains numerous proprietary software packages which, by legal agreement with vendors, require protection.

PROJECT CONSTRAINTS

The constraints imposed on the project during its seventeen month life were similar to the constraints confronting any organization. They are cited here to reassure the reader that the project was executed in a site with real-world people, time schedules, budgets and conflicting priorities, not in a laboratory in the environment of a university or "think tank."

Some of the project constraints were:

- Stability and Reliability

The MID's major objective is to provide a stable and reliable computer operating environment for the agencies which it serves. The implementation of the project was necessarily scheduled over a long enough period of time to avoid adversely impacting the stability of the systems in the MID data center.

- Cost to Data Centers Users

The MID uses a complex chargeback system whereby each user agency is billed monthly for the actual computer resources used in processing its jobs. The agencies use this historic information to project future costs and develop their budgets. Consequently, the overhead costs resulting from the use of the Resource Security System (RSS) could not be passed on to data center users.

- MID Software System Installation Philosophy

The task of installing RSS was further complicated by a long-standing MID philosophy regarding the application of Program Temporary Fixes (PTFs). The diversity of applications processed at the data center requires the application of all available PTFs to any change of or extension to the operating system (OS/MVT) prior to installation. This meant that the compatibility of all PTFs with RSS had to be assured.

- Conflicts with User Information System Development Plans

The impact of the implementation of major new application systems was not adequately planned for by the project. Although users were apprised of the software implementation schedule, users did not voluntarily reciprocate by supplying the project with their system development plans. This oversight caused some scheduling and resource allocation problems.

- Future Availability of RSS

The Resource Security System is not available or supported by IBM after January, 1974. It was installed on a test site basis as a prototype to enable the State of Illinois and IBM to plan their respective future software security requirements.

- Hardware Considerations

The hardware configuration changed a number of times during the course of the project. The affect of these changes on the project's performance measurement activities is discussed in Appendix E.

- Administration Change

Finally, the project was executed during the transition period from a Republican to a Democratic administration. Although top management in both administrations supported the project, changing policies and priorities caused substantial delays and resource allocation problems. A number of newly appointed user operating managers who were pressed for immediate changes by the new administration did not look favorably on the project. Project relations with these managers remained strained throughout the life of the project.

PROJECT EXCLUSIONS

It became obvious during the course of the project that the capability to secure fields and records within a file was desirable. Although the RSS provides this capability, only data set level security was installed. Therefore, the costs of implementation and operation of RSS do not address the subject of field and record level security.

The RSS was designed to co-exist only with the MID's existing teleprocessing control systems. No additional security has been provided for these systems. RSS security affected only the batch and remote job entry systems even though it provided a teleprocessing interface. However, administrative controls for teleprocessing are addressed.

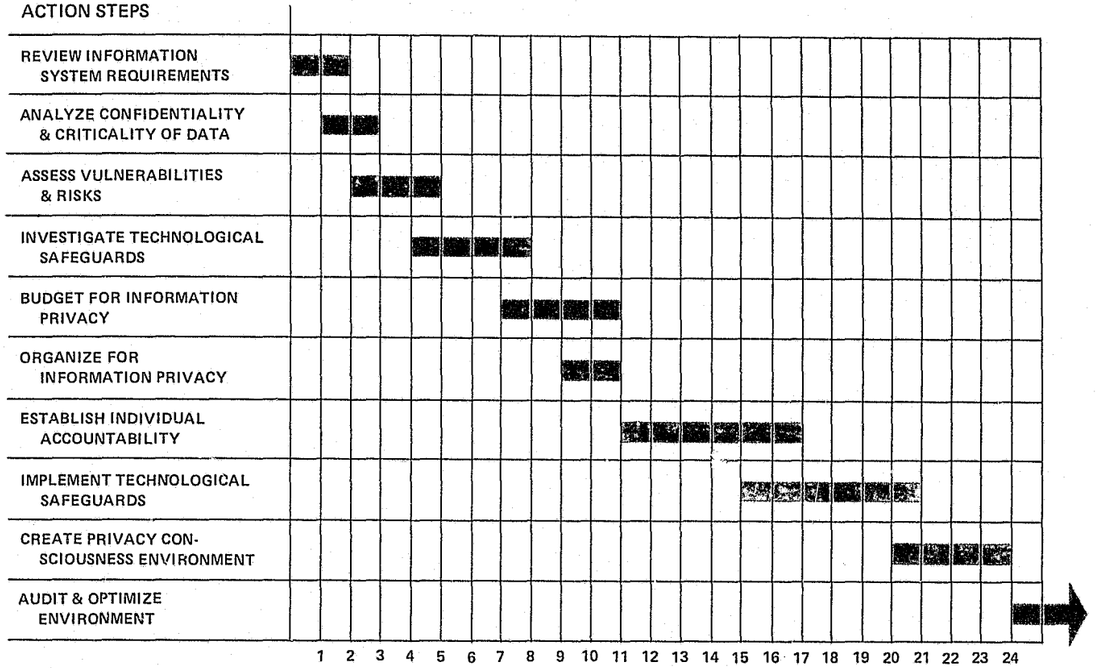
Finally, the project did not address the evaluation of hardware security devices in any depth. There are, therefore, no comprehensive conclusions made concerning the pros and cons of incorporating various security checks as hardware versus software functions.

CHAPTER II: A FRAMEWORK OF CONSIDERATIONS

Like most organizational objectives, information privacy cannot be achieved without management commitment to a well-defined plan of action supported by appropriate resources. Consideration of such a plan should initially arouse three basic questions in your mind:

- **WHAT SHOULD BE DONE?**
- **WHO SHOULD DO IT?**
- **HOW WILL I KNOW WHEN — AND IF — IT IS DONE CORRECTLY?**

Because specific security and privacy programs are organization-dependent, it would be presumptuous to try to prescribe a universal panacea. Specific security implementation plans for information systems depend on a number of factors including the size of the organization, the pre-existence of security safeguards, the functions performed by the organization and many others. However, information privacy programs can be characterized by a number of similar action steps. These steps comprise a generalized information privacy action plan as illustrated on the next page. An arbitrary time schedule has been imposed as a frame of reference to indicate that security and privacy programs are not implemented overnight — they cost time and money.



A GENERALIZED INFORMATION PRIVACY ACTION PLAN

ACTION STEP ONE: REVIEW INFORMATION SYSTEMS REQUIREMENTS

- What data is being collected?
- Who needs this data?
- Why do they need it?
- When do they need it?
- Are all new uses of data being cleared through you?
- Are all new items of data collection cleared through you?

ACTION STEP TWO: ANALYZE CONFIDENTIALITY AND CRITICALITY OF INFORMATION

- How complex should your information classification structure be? (i.e., How many levels of security are required?)
- What guidelines are available to assess the value of information?
- What are your legal and social responsibilities regarding information privacy?
- How much protection is required for each kind of information?

ACTION STEP THREE: ASSESS VULNERABILITIES AND RISKS

- What specific vulnerabilities confront the organization's information systems and resources?
- What is the risk of an accidental or intentional disclosure, modification or destruction of information given existing safeguards?
- How much could the risk be reduced given an increase in the amount of security protection?
- How do you assess the tradeoffs between increased security and increased cost?

ACTION STEP FOUR: INVESTIGATE TECHNOLOGICAL SAFEGUARDS

- What technological safeguards are presently being used by the organization?
- How is the organization keeping abreast of new technological developments to provide a more cost effective mix of safeguards?
- What are the costs associated with available technological safeguards?
- What safeguards are similar organizations using?
- How effective are available technological safeguards?

ACTION STEP FIVE: BUDGET FOR INFORMATION PRIVACY

- What are the costs involved in the implementation and operation of a security and privacy program?
- What computer costs are billable to information systems users and what costs should be absorbed into the overhead of the computer system?
- What is the value of information privacy and security to the organization?
- How can you maximize security given budgetary constraints?
  or
- How can you minimize your cost given a specific security requirement?
- Who will pay for increases in user processing costs during implementation?

ACTION STEP SIX: ORGANIZE FOR INFORMATION PRIVACY

- What general functions are affected by the information privacy organizational objective?
- What new staffing is required?
- What qualifications are required to fill these roles?
- How will the information system security function be incorporated into the organization structure? Staff or line? Centralized or decentralized?

ACTION STEP SEVEN: ESTABLISH INDIVIDUAL ACCOUNTABILITY

- Who has the need to know, the need to change and the right to expunge information?
- Why do they need to know?
- When do they need to know?
- Have these individuals received security clearances?

ACTION STEP EIGHT: IMPLEMENT TECHNOLOGICAL SAFEGUARDS

- What is the priority of the information privacy objective in relation to other organization objectives (e.g., production, efficiency, other projects, etc.)?
- How will the implementation of an information system security and privacy program impact user information system development plans and vice versa?
- How much and what kind of vendor support will be required to implement new technology?
- What additional resources (e.g., people, computer time, etc.) will be required during the implementation?
- Who is responsible for periodically communicating project status and plans to the information system user community?
- Where is the implementation plan?

ACTION STEP NINE: CREATE PRIVACY CONSCIOUS ENVIRONMENT

- Do organization policies address the information privacy problem?
- Are the required substantive procedures well-documented, understood by all concerned parties and enforced?
- Is your present program of education sufficient to induce changes in behavior?
- Do you evaluate individuals based on their information privacy responsibilities?

ACTION STEP TEN: AUDIT

- What is the mix of talents required for an effective auditing team?
- Have all the organization's vulnerabilities been identified?
- How effective is the existing mix of technological and administrative safeguards?
- Does the existing security environment satisfy the organization's legal and social responsibilities?
- What improvements can be made to make security more efficient and effective?
- What is the frequency of your auditing procedure?

Clearly, the information privacy problem involves activities in four distinct disciplines — legislation, education, administration and technology. Each organization must develop a well-balanced approach to the problem within its resource constraints — assessing the tradeoffs between the organization's need for information on the one hand and the elements and economics of security and privacy on the other.

CHAPTER III: THE ELEMENTS OF SECURITY

Information privacy and data security programs can be structured by considering four dependent functional elements.

- **Security Administration**
- **Information Privacy and Security Education**
- **Technological Requirements & Considerations**
- **Legislative Considerations**

As an information systems manager, your objective is to develop a balanced and practical approach to security. To meet this objective, you will need a complete understanding of the technological, administrative, educational and legal requirements for security and privacy in information systems.

SECURITY ELEMENTS / ACTION STEPS	SECURITY ADMINISTRATION	INFORMATION PRIVACY & SECURITY EDUCATION	TECHNOLOGICAL REQUIREMENTS	LEGISLATIVE CONSIDERATIONS
REVIEW INFORMATION SYSTEM REQUIREMENTS	●			●
ANALYZE CONFIDENTIALITY AND CRITICALITY OF DATA	●			
ASSESS VULNERABILITIES AND RISKS	●			
INVESTIGATE TECHNOLOGICAL SAFEGUARDS			●	
BUDGET FOR INFORMATION PRIVACY	●			
ORGANIZE FOR INFORMATION PRIVACY	●			
ESTABLISH INDIVIDUAL ACCOUNTABILITY	●			
IMPLEMENT TECHNOLOGICAL SAFEGUARDS	●		●	
CREATE PRIVACY CONSCIOUS ENVIRONMENT	●	●		
AUDIT & OPTIMIZE ENVIRONMENT	●	●	●	●

■ INFORMATION PRIVACY AND DATA SECURITY IS AN INTERDISCIPLINARY PROBLEM

SECURITY ADMINISTRATION

The generators, operators and users of information systems play the most important role in a successful information privacy and security program. Security administration must be governed by a continual awareness of the functions created or affected by information privacy objectives. There is an on-going need for the communication of appropriate policy, the development and enforcement of substantive procedures and the administration of an on-going program of education.

Security should be a line management responsibility equal in importance to system reliability and efficiency. This requires integrating a wide range of security functions and responsibilities into the organization structure. Specifically, the following list indicates some of the functions with which you must be concerned.

- **Technology research** is the responsibility of the hardware/software planning group. An awareness of the state of the art in security technology is no less important than an awareness of the most efficient and effective technology affecting other parts of your operations.

- **Administration of a software security system** includes several related activities:
  Classification of files and file linkages using the guidelines established by user policymakers.
  Identification and authentication of resources (e.g., volumes, terminals, files, transactions, programs, personnel) by general systems and operations management, and authorization to access confidential and critical resources again using the guidelines prescribed by user policymakers.

- **Education** of all management, supervisory and operating personnel is necessary to achieve an on-going "security and privacy consciousness" within the organization. The responsibility for the development, implementation and operation of a security education and training program resides with general administrative management.

- **Security auditing** can be performed by internal or external auditing staffs. The focus of the audit should be directed toward security of the:
  Environment surrounding the computer,
  Application and software systems within the computer and
  Interfaces between the computer system and its environment.

- **Design and programming security** is a systems management responsibility. Security concern must be built into each phase of the system development life cycle, including:
  Project Initialization
  Investigative Study
  Generalized Systems Design
  Detailed Systems Design
  Implementation Planning
  Systems Implementation
  Post Implementation Evaluation

- **Data center operating environment security** is essential to safeguard confidential and critical information and includes the following considerations:
  Secure operating practices to control input, processing and output at every data center work station.
  Safeguards to assure software and application program integrity and to control access to information.
  Backup provisions to minimize service interruptions to users in the event of a disaster or disruption.
  Certification procedures to assure the existence and execution of adequate security practices.

  Enforcement of policies and procedures must be accomplished at all levels of the organization. This responsibility includes:
  Determining practices and procedures for breaches of security by employees, and
  Developing investigation procedures for security violations or privacy grievances presented by data subjects.

- **The Security Office** may come into existence as part of this program. Development and implementation of a security program may require the formation of a project team. Many of these functions can be executed more efficiently and consistently if another entity — called the security office — is added to the organizational structure. This addition assists, but does not replace, the security responsibilities of line management.

- **Administration of the on-going security program** (including coordinating all security related activities, budget preparation, policy and procedural review and development, etc.) is a general administrative management responsibility. Since successful on-going security and privacy programs are people dependent, organization policy and procedures must communicate the attitudes and convictions of senior management throughout the organization. Specifically, policy statements are required to address:

  Data gathering — To ensure that only that information which is necessary to execute a legislated program or an approved corporate endeavor is collected.

  File contents — To ensure that adequate controls are used to maintain the accuracy, completeness, relevance and timeliness of data.

  Data Storage and Handling — To ensure that:
  Adequate controls are used to maintain the accuracy, completeness, relevance and timeliness of data,
  Procedures are understood for acts of negligence or carelessness,
  Information is protected against loss.

  Data dissemination — To limit the distribution of information to authorized users.

  Access control — To ensure that only those individuals with a need to know, need to change or right to expunge data have access to the data — either physically or via computer software. This control is manifested in the development of a security profile which defines accessability to all system resources.

Personnel — To ensure that:
All applicants for "sensitive" positions are properly screened,
Responsibilities are clearly defined,
All employees agree with the organization's Code of Conduct.

Audit responsibility — To ensure that periodic checks on the efficiency and effectiveness of all administrative and technological safeguards are executed.

Organization — To establish a physical manifestation of your concern by organizing and committing resources to the information privacy objective.

The working tools of the security program are the substantive **procedures** which are necessary to translate management policy into action-oriented security practices. The following pages provide an outline of the contents of a manual of *Recommended Security Practices* which was developed for the Management Information Division. This manual should provide a useful reference for you and your staff.

RECOMMENDED SECURITY PRACTICES

General Introduction and Administration of the security program including:

- A review of the federal and state legislation concerning information privacy and its implications on the data center's security responsibilities.
- Management policy statements on the subject of security and a Code of Conduct for all state data processing employees.
- Work flow controls
- Personnel practices

Change Control Security Measures including:
- Planning and control of hardware changes to assure compatibility with installed security measures.
- Planning and control of software changes to prevent inadvertent loopholes in existing security software.
- Control over changes to the physical plant to prevent disruption of security controls and to avoid exposure to damage.
- Control over system documentation and changes to software and application programs to prevent unauthorized alteration or penetration.

Software Related Security Measures including:
- Classification of information, identification and authorization of resources and maintenance of security profiles.
- Handling of attempted violations.
- Identification of optional software security features.
- Explanation of the real time audit functions and responsibilities of the software security system.
- Procedures for providing control of systems documentation and changes to software and application programs.

Terminal Access Related Security Measures including:
- Approaches to provide security of computer terminals and confidential terminal output.
- Controls over access to computers and files.
- Techniques to reduce vulnerability to data loss or access via communications lines, modems and junction points.

Systems Design Related Security Measures including:
- Analysis of the system information requirements relative to the need for and use of the information.
- Techniques for designers and programmers to build security into new information systems.
- Logical review points in the systems development life cycle to audit the security features of a new system.

Physical Plant Related Security Measures including:
- Procedures for the authorization, issuance, and retrieval of employee identification.
- Access controls and disruption prevention within the building housing the data center.
- Physical security measures to be observed in all data processing work areas.
- Provision for data, equipment and facilities backup.
- Contingency plans to minimize disruption loss and to facilitate recovery of services.

A Security Auditing Checklist

A Glossary of terms referenced throughout the manual

The *Recommended Security Practices* manual is intended to:
Describe available safeguards and what they are designed to prevent or detect,
Describe how the safeguards are to be used,
and
Define the specific responsibilities required for successful execution and enforcement of the security program.

This combination of management policy statements and well-documented, enforceable procedures is intended for the individual responsible for handling confidential or critical information. The manual will provide him or her with a convenient reference to your organization's posture on information privacy and security as well as a clear definition of his or her security-related job responsibilities.

INFORMATION PRIVACY AND SECURITY EDUCATION

No technology for security, no matter how cleverly constructed, can operate effectively unless the people involved are committed to securing their system. To ensure this commitment, the people involved in developing, operating and using information systems must be aware of the importance of protecting the privacy of information as well as their specific responsibilities related to the privacy and security problem.

One target group for education is, of course, the people involved in the function of electronic data processing. These people can appear within an institution which furnishes its own EDP services, or they can be found in institutions whose entire function is the automated processing of information. In either case, the *information technologists* (generators and operators of automated information systems) provide a service to a **user** client. The users of information systems, then, are the other target group for an education program.

In most cases, the user agency is the source of substantive decisions about the information system. So, a secure information system depends fundamentally on the commitment of the system's users. The user decides what information he or she wants, in what form, and how and when the information is to be used. Since these decisions are most frequently based on goals and policies of the institution, it would be impractical to rely on the information technologist to make fundamental decisions about the information system, including its impact on the value of personal privacy.

Most information systems contain substantial operations where data processing is still carried out manually and in the form of English, hard copy records. These manual operations are as significant to the problem of creating a secure information environment as are the automated operatations. Procedures in the manual area are frequently simply carried over into EDP without any examination of the implications of such a transfer.

THE PURPOSE OF EDUCATION

Education of a user agency or department creating a concern for privacy and providing the user with the tools necessary for maximizing the protection of privacy within the institution. At the same time, however, you must avoid conflicts with the valid functions of the information system. Specifically, your goals are to:

- Raise the level of user awareness
  The user must be made aware of his or her responsibility for the privacy of information. Most institutions exist for specific purposes, and they develop an information system to serve those ends. They are not eager to add an additional concern which they feel is outside their area of responsibility.

- Ensure the user understands the need for balance between the organization's information requirements and the right to privacy

  An information system by its very nature has the effect of infringing on the area of privacy. There is a requirement for information to be gathered, used, transmitted and stored and the urgency of this requirement often overshadows any concern for the rights to privacy of the individuals supplying the information.

- Develop applicable solutions
  A user department must develop its own practical avenues to increase the privacy of its information system. Even though such knowledge can be found in the hands of experts who have studied the area, an outside expert cannot know the specific processes and problems of each department. It remains for the insiders to decide how the interests of privacy can best be made compatible with their own organizational goals.

- Provide avenues whereby users and information technologists can interact on the subjects of privacy and security
  Under these circumstances, both parties can define responsibilities for privacy and use all possible methods for its protection.

AN APPROACH TO EDUCATION

An operating assumption of your education program must be that individuals who are generators of new information systems or are responsible for maintaining existing systems have a full consideration of the privacy rights of the data subjects. A further assumption must be that with the current and trending technical, legal, social and political issues and concerns related to individual privacy, this fundamental obligation will continue to exist and may become even more important in the near future.

With these assumptions in mind, the following educational approach presents the current best thinking about designing and operating information systems with maximum privacy protection.

- Initiation and Sanction
  Ideally, information systems procedures will contain specification for periodic review of the privacy consciousness of the system as well as assigned accountability for that review. In any case, top management sanction is desirable, and the program recommends that a proposed review be initiated by a briefing of the executive officer.

- The Design Group
  A design group is ideally composed of three to five managers including representatives of both user and EDP departments. The responsibility of the Design Group is twofold: to aid the individual manager in planning the implementation steps of review and analysis appropriate to the target system and to serve as critic and support for changes in the information system.

- Manager/Work Unit
  The information system manager should retain direct implementation responsibility for the results of the review. Operating personnel of the system, however, will also have information necessary for an effective review, and acceptance of the necessary modifications in work practices and habits will be highly dependent upon operating personnel understanding the need for these changes. The following approach is offered as one way of effecting this attitude. Your manager, with Design Group Counsel, may necessarily adapt this approach to fit your particular organization.

Step 1. At the initial meeting of work unit personnel.
- share and confer on the management directive and discuss its purpose.
- view videotape, *Whose Right To Know.*
- discuss how the tape relates to your work unit.
- discuss next steps.

Step 2. Complete the descriptive Information Systems Analysis Flow chart (Appendix A) (manager with aid of selected work unit personnel and EDP manual data processing personnel as needed).

Step 3. Review the flow chart with the Design Group, applying the Privacy Criteria (Appendix B).

Step 4. At the second meeting with work unit personnel.
- view videotape, *Follow That Card!*
- review the flow chart/privacy criteria analysis.
- generate suggestions and recommendations for improvement.

Step 5. Review data with the Design Group and prepare report for Management, including:
- general findings.
- operational changes implemented.
- policy and procedure changes recommended.

Step 6. Implement changes Management approves.

Step 7. Review the process with the Design Group.
- experience with the first (pilot) information system.
- determine a follow-up schedule and procedure.
- select the next systems for review/analysis.

As a result of this process, you should be able to make some observations, such as:
- The individuals involved in the information system do not know **what** is expected of them. In which case, work clarification is indicated.
- The individuals involved do not know **how to do** what is expected of them. Job Training is indicated.
- The individuals know what and how to perform a function but seemingly do not **want to** perform. Performance problems of this kind are the most difficult to deal with. Some form of counseling is normally required.
- Other potential problems which may surface include:
  priorities are unclear.
  misallocation of work assignments is creating unrealistic workloads.
  system design is inadequate for current purposes, needs and requirements.
  management performance expectations of individuals are too low.

The educational program described above should enable the manager, with Design Group and work unit help, to determine what is needed to upgrade the security aspects of the information system. Such a systematic review may also disclose opportunities for upgrading the efficiency and effectiveness of the work operations involved. The improvement needs and appropriate management responses will, of course, be unique to each system.

THE PROCESS OF EDUCATION

- Initiating the Process

Most institutions begin to initiate change through a sanction from the top level of the organization. Thus, the process of creating a concern for privacy begins with the education of the top executive. An executive overview* which outlines the social, legal, economic and ethical justifications for a concern for privacy in information systems as well as a plan of action should be submitted to the top executive.

The first videotape of this education package, *Whose Right To Know,* demonstrates the real and potential impact of such a system on individuals and the society at large. Viewing this videotape can be an important part of the executive's education, whether to gain his support and sanction or merely as a matter of course as with the proposal of any new information system.

A meeting should then be arranged with the executive and the persons most knowledgable about the general operations of the institution for the purpose of planning the general scope and nature of the privacy program. At this meeting, the executive and assistants will designate a group of employees who are closely involved with the existing or proposed information system or systems. This group will thereafter serve as a "Design Group" for the education program.

The Design Group will gather information about the area of concern, decide what types of changes or initiatives are required, verify the policy commitments or changes with the executive and implement them at the operational level. Thus, ideally, the Design Group should be comprised of people of authority in order to obtain the necessary information about their own operations, to integrate the new information about privacy provided in the education program, and to implement changes or institute safeguards required by the comparison between their existing operations and an ideal model of a privacy protective system. Inclusion of a representative of the EDP function within the information system in the Design Group should provide for better communication between the user and his technical support.

- The Design Group as an Information Gathering Entity

Step 1. Introduce the Design Group to the Project.

Optimally, the Design Group will function both as a group and as individuals responsible for specific areas of concern. Thus, once the group has been selected by the Executive or an assistant, the program should be initiated by a Group meeting, attended by the Executive or Assistant Executive, in order to explain the goals of the program. At the initial meeting, the Design Group may view the videotapes one and two (*Whose Right To Know* and *Follow That Card!*) These modules create an awareness of the problems involved in information systems and demonstrate the potential for instituting privacy protective measures. The videotape programs will start the Group thinking of the types of situations they may find within their own institution.

Step 2. Gather Specific Information About Operations

At the first meeting, the Design Group should be presented with a Questionnaire (Appendix D). If properly used, this tool will provide a general picture of the information system or systems existing or projected to be within their area of responsibility. Design Group members will use this questionnaire to familiarize themselves with the information systems aspect of their operations as they gather information from subordinates.

*See *What Every Executive Should Know About Privacy in Information Systems*

Once each questionnaire has been filled out, (this may involve several questionnaires for each Group member), the Design Group member is ready to transfer the information gathered onto a flow chart, which will portray the path of information through his proposed or existing system or systems. Most likely, in attempting to transfer the information from the questionnaire to the flow chart, the Group member will want to meet again with his subordinates. This second meeting with subordinates gives them an opportunity to voice additional concerns and interests which may have arisen since the videotape program and the questionnaire directed their attention to the information privacy problem.

In the case of a new system, the questionnaire can serve the function of defining the information needs of the institution, and the flow chart of the projected system may show whether the system will satisfy those needs.

- The Design Group as an Analytic Entity

Since an information system almost inevitably involves physical entities — people, forms, file cabinets, computers, teleprocessing terminals — which exist and move in space and time, the flow chart can guide the Group member to the various points in his organization where information is likely to be handled and to the decision-making stations along the flow of information. Thus, the flow chart should aid in visualizing the privacy implications of such systems in operation.

Once the existing or projected information system is laid out in flow chart form, the Design Group member may proceed to analyze the system with reference to the Generic Privacy Critera (Appendix B). The Privacy criteria are closely related to the flow chart, and the Group member should be able to measure the actual practices, as described or projected along the flow chart, against the options for a more privacy-oriented system presented by the Privacy Criteria.

Roughly, the Privacy analysis breaks down into six areas of interest:

Interest area 1: Systems Development

A system should be analyzed at the starting line — development. The criteria and the reference materials classified according to the criteria are most useful to the Group member and/or executive at the time a new information system is proposed or an existing one reviewed for modification. At this stage protective procedures and policies may be instituted, which will involve substantial saving if such changes can be projected rather than added at a later date. Such considerations as the limitation of the system to clearly defined purposes, the inclusion of privacy in the management system, the education of the operative personnel involved and provision for some deference to the right of the subject may be built into the system at this time. It is recommended that each Group member consult at this stage of the analysis with the EDP Design Group member about projected systems, since the input of this member may be particularly useful at this point.

Interest area 2: Data Collection

The Privacy Criteria call for serious attention during the early stages to Data Collection. One of the more serious criticisms directed at information systems which include electronic data processing capabilities is their capacity for maintaining an almost unlimited amount of information, once it is collected. Such a problem can be solved most easily by minimizing the collection of data.

Interest area 3: Data Transmission

Privacy concerns in the area of the transmission of information can occur at several points along the information flow. However, the requirements for secure and rapid transmission probably apply fairly uniformly regardless of where the process of transmission is taking place.

Interest area 4: Administrative Handling

This is probably the stage at which changed attitudes through education can be most helpful, since even the most sensitive of information seems neutral if it is processed in the routine of a person's job. Studies of information systems have revealed that privacy is best protected when the information system is developed with a sense of *esprit de corps* with regard to its special nature, and this sense is probably the most important product of the initiation of privacy protective procedures.

Interest area 5: Dissemination

From a privacy standpoint dissemination of information may be improved in two general ways. First, by carefully considering the persons or institutions entitled to receive information. This is obviously best handled at the design stage of the information system. Secondly, by carefully considering the technical, physical and legal safeguards which may be placed around the entire information system to avoid unwarranted incursions.

Interest area 6: Storage and Destination

An information system is probably most vulnerable to destruction of privacy through intrusion at the stage of storage — either temporary or permanent. Here again, the concern about the storage and retrieval potential of electronic data processing is applicable. For this reason, the privacy criteria place heavy emphasis on an analysis of the destination of information and its speedy expungement.

At each stage along the flow chart, the Group member may refer to the materials indexed under the privacy criteria for general guidelines to acceptable practices. He can also find there examples of the manner in which problems similar to his have been handled in other systems. At this point in the education process, the Design Group member may become something of a privacy co-ordinator. It may seek out the advice of subordinates through discussion to find ways in which they can alter or improve their procedures. People at the system operating level should be exposed to the second videotape program, *Follow That Card!* This will help the Design Group member develop recommendations for operational and policy changes within the projected or existing system.

- The Design Group and Policy and Operational Changes

After analyzing the information system, the Design Group members should be ready to make policy change recommendations. They should also be prepared to submit operational changes or procedures which would be generated by the new policy. Of course, some changes may be implemented within existing policy. Policy changes will have to be referred back upward to the policy-making executives.

Before such recommendations are made, it would be fruitful for the Design Group to meet again as a group to compare their experiences. They may find sufficient similarity to justify joint recommendations. These would apply across systems, thus simplifying the implementation procedure and avoiding overlap. At this same meeting, the EDP Design Group member may have substantial input regarding existing and projected technology.

A meeting with the executive level would add executive sanctions to whatever policy and operative changes are recommended. Changes in policy must be communicated to the lower levels of the institution through channels, and the flow chart analysis should expedite this undertaking by defining the groups of operating personnel to whom specific changes would apply. The operational changes can then be implemented. At this point, the relevant modules of the Videotape Program will be most useful. For purposes of preparing the operational personnel for changes in their procedures within the user agency, the second module, *Follow That Card!*, will serve two purposes. (If the group of workers has not viewed videotape one, *Whose Right To Know*, this tape should precede the viewing of Videotape #2.) One, as a consciousness raising device. Two, as a means of familiarizing each group of workers along the flow chart with the reasons for the new demands being made upon them. Where the user agency is responsible for its own electronic data processing, or where the altered procedures require changes in the computerized elements of the data system, the following videotapes are available:*

Videotape #3 — *Implementing the Information Privacy and Security Program.*

Describes the steps, considerations and responsibilities involved in developing and implementing an information privacy and security program.

Videotape #4 — *Administering the Information Privacy and Security Program.*

Describes the organizational and administrative implications of an information privacy and security program.

Videotape #5 — *Designing Privacy and Security Into Information Systems.*

Describes the considerations involved in designing and developing information systems with privacy and security in mind.

Videotape #6 — *Software Security and Terminal Access Concepts.*

Describes the fundamental characteristics of a software security system and the considerations involved in securing telecommunication networks.

Videotape #7 — *Physical Plant Security.*

Describes the considerations involved in providing physical protection for information systems.

Videotape #8 — *Back-up Security.*

Describes the considerations involved in providing adequate backup capabilities for information system resources.

Videotape #9 — *What Every Executive Should Know About Privacy in Information Systems.*

Presents the concepts of the need for and scope of the installation of an information privacy and security system from the executive's viewpoint.

*A brief outline of the objectives and pertinent points covered by each videotape is included in the *Session Leader's Guide, SAFE Videotape Training Sessions.*

The Design Group should conclude its most active phase with a report back to the Executive regarding their whole undertaking. This report should include the implementation of new or changed policies and procedures.

FOCUSING ON EDP REQUIREMENTS

The technical and administrative requirements that apply solely to EDP personnel are merely an extension of the overall education process. The education program developed to assist in the discharge of these security responsibilities is directed toward personnel with a diversity of functional data processing responsibilities and is comprised of several elements. The chart on the following pages outlines the overall approach taken to provide security education to data processing personnel with a wide range of skill specialties. As the exhibit displays, a number of methods and media are employed as appropriate for the subject matter.

MANAGEMENT INFORMATION DIVISION

SECURITY EDUCATION PROGRAM

Security Program Content Description	Training Approach and Media						Types of Personnel To Receive Training										
	Administrative Training			Technical Training													
Section / Subsection / Element	Admin. Procedures	Formal Training	Supervision	Technical Procedures	Formal Training	Supervision	Computer Operators	Scheduling and Librarian	Input/ Output Control	Data Conversion	Project Managers	Senior Analysts	Application Programmers	Data Base Specialists	Communications Specialists	Software Systems Support	Security Office Personnel
I. General Introduction																	
A. Philosophy and Reasons for the MID Security Program	x	x	x				x	x	x	x	x	x	x	x	x	x	x
1. Individual Right to Privacy																	
2. Security Vulnerabilities and Problems																	
3. Inform Personnel of their Responsibilities																	
4. Create General Awareness of Security Program	x	x	x				x	x	x	x	x	x	x	x	x	x	x
B. Information Privacy and the Law	x	x	x				x	x	x	x	x	x	x	x	x	x	x
C. Applicable Policies, Directives and Code of Conduct	x	x	x				x	x	x	x	x	x	x	x	x	x	x
D. Categories of Security Exposures																	
1. Accidental Disclosure																	
2. Intentional Infiltration																	
3. Loss of Data																	
4. Erroneous or misleading information																	
5. Absence of established standards																	
E. Interdisciplinary Approach	x	x	x				x	x	x	x	x	x	x	x	x	x	x
II. Agency User Security																	
A. Introduction to Agency Security Responsibilities		x	x								x	x					
B. Exposures to Risk in Manual Processing Operations		x	x								x	x					
C. Typical Security Safeguards		x	x								x	x					
III. Security Administration																	
A. Organizing for Security	x	x					x	x	x	x	x	x	x	x	x	x	x
B. Security Implementation Plans	x	x					x	x	x	x	x	x	x	x	x	x	x
C. Administrative Work Flow Control	x	x	x				x	x	x							x	x
1. I/O Control																	
2. Console Operator																	
3. Production Control																	
4. Tape Work Stations																	
5. Disk Work Stations																	
6. Printer Work Stations																	
7. Librarian																	
8. Shift Supervisor																	
9. Security Console Operator	x	x	x				x	x	x		x	x				x	x
D. Personnel Practices																	
1. Screening																	
2. Bonding																	
3. Work Practices																	
4. Rotation and Backup																	
IV. Change Control	x	x	x				x	x	x						x		x
A. Facility	x	x	x				x	x	x					x	x	x	x
B. Hardware	x	x	x				x	x	x		x	x	x	x	x		x
C. Software	x	x	x				x		x		x	x	x	x	x	x	x
D. Documentation and Program																	
V. Software Security	x	x	x	x	x	x	x	x	x							x	x
A. Access Control and Authorization																	
1. Identification of Resources																	
2. Classification of Information																	
3. Authorization of Users																	
4. Security Profile Maintenance	x	x	x	x	x	x	x	x	x							x	x
B. Handling of Attempted Violations	x	x	x	x	x	x											
C. Additional Software Functions																	
1. PURGE Options																	
2. Software System Integrity																	
3. Operating System Validation	x	x	x	x	x	x											x
D. Real Time Software Auditing																	

Security Program Content Description	Training Approach and Media						Types of Personnel To Receive Training										
	Administrative Training			Technical Training													
Section / Subsection / Element	Admin. Procedures	Formal Training	Super-vision	Technical Procedures	Formal Training	Super-vision	Computer Operators	Sched-uling and Librarian	Input/ Output Control	Data Conversion	Project Managers	Senior Analysts	Application Programmers	Data Base Specialists	Com-munications Specialists	Software Systems Support	Security Office Personnel
VI. Terminal Related Security																	
A. Access to Terminals and Output	x	x	x								x	x	x	x	x		
1. Terminal Location																	
2. Computer Terminal																	
3. Terminal Output	x	x	x		x												
B. Access to Computers and Files											x	x	x	x	x		x
1. OS/RSS																	
2. CICS																	
3. IMS																	
4. HASP	x	x	x														
C. Access to Communications Lines															x		
1. Junction Points and Modems																	
2. Information Encryption																	
3. Communication Line Service Classes																	
VII. Systems Design Security																	
A. Project Initialization	x	x	x								x	x	x	x	x		
B. Investigative Study	x	x	x								x	x	x	x	x		
C. Generalized System Design	x	x	x								x	x	x	x	x		
D. Detailed System Design	x	x	x								x	x	x	x	x		
E. Implementation Planning	x	x	x								x	x	x	x	x		
F. Systems Implementation	x	x	x								x	x	x	x	x		
G. Post Implementation Evaluation	x	x	x								x	x	x	x	x		
VIII. Physical Plant Security	x	x	x		x	x											
A. Identification of Personnel							x	x	x	x	x	x	x	x	x	x	x
1. Data Processing Employees																	
2. Non Data Processing Employees																	
3. Contract Personnel	x	x	x			x											
B. Office Building Security							x	x	x	x	x	x	x	x	x	x	x
1. Identification/Authentication																	
2. Visitor Logging																	
3. Restricted Access	x	x	x			x											
C. Data Processing Security							x	x	x	x	x	x	x	x	x	x	x
1. Control of Access																	
2. Input/Output Controls																	
3. Information Disposal																	
4. Hazard Control																	
IX. Backup and Contingency Planning	x	x	x	x													
A. Backup Practices											x	x		x			
1. Information File Backup																	
2. Documentation Backup																	
3. Equipment Backup	x	x	x	x													
B. Contingency Planning							x	x	x	x	x	x	x	x	x	x	x
1. Emergency Situation Actions																	
2. Provision for Alternate Processing of Work Loads																	
3. Software Recovery																	
4. Equipment Recovery																	
5. Facility Recovery or Replacement																	

Administrative training concentrates on the "what"and "who" of the security program by specifying the safeguards to be administered and the personnel responsible for specific security functions. Administrative training includes the following elements:

- Formal training is conducted with videotape presentations which have been developed from scripts based on the security practices manual. The first two modules are general introductions to information privacy and security and are intended for presentation to all data processing and user audiences. The remaining six information system related modules each treat a specific element of the security program. The videotape sessions are designed so that personnel with specific functional interests need attend only those sessions applicable to their areas of responsibility. Finally, the *Executive Overview* module is intended for executive audiences and provides a broad brush treatment of the information privacy problem and its implications to most organizations.

- Supervision is on-the-job reinforcement and explanation of the material presented in the first two training elements.

Technical training focuses on the "how" of the security program by explaining in detail the manner in which each safeguard is to be implemented and operated. Technical training includes the following elements:

- Technical procedures are desk instruction level procedures which detail each step to be taken in the operation of a specific safeguard. Examples of technical procedures include the physical access control badge issuance and maintenance procedures, the security office procedures for handling attempted violations and the detailed contingency planning procedures.

- Formal training is conducted in a classroom mode with training sessions presented by vendors or training programs developed within the Management Information Division.

- Supervision is the technical instruction and follow-up conducted at the work station to assure that each safeguard is being properly administered.

The mix of training elements developed in this security program is specifically appropriate to the information systems environment in the State of Illinois. Approaches to security training will clearly vary from organization to organization, but some of the characteristics of this program are noteworthy.

- The education material is **informative**. It explains why there is concern for information privacy and security, what exposures confront the organization and what technological and administrative safeguards are to be used.

- The education approach is **multi-media**. This is necessary to stimulate and maintain interest and concern.

- The education modules are **selective**. Each module is intended for a specific audience.

- The education program is **continuing** to assure an on-going level of security consciousness.

TECHNOLOGY REQUIREMENTS & CONSIDERATIONS

The executive or administrator has a wide range of technological alternatives to consider in the development of an information privacy and data security program. Specifically, three important questions must be considered:

- What kinds of technological safeguards are available to provide information privacy and data security?
- What are these safeguards designed to protect and how effective are they?
- How should you determine which specific safeguards to select for your security system?

As data flows through the organization, various security requirements become evident. Physical safeguards are necessary to protect data throughout its manual processing and storage phases. However, once data enters the automated data processing phase, additional technological safeguards play an important role. These technological safeguards can be conveniently separated into three major categories:

- Software Security
- Hardware Security
- Physical Security

At present, the security capabilities of these technological tools have not been fully developed. Users and manufacturers of hardware and software systems share responsibility for this situation. The following pages describe the desirable capabilities and qualities of these systems — regardless of whether these capabilities exist in the present state of the art.

SOFTWARE SECURITY

Introduction

The computer operating system was developed to alleviate many of the repetitive and time-consuming actions involving data processing personnel. Acting as the interface between man and the computer, present day operating systems are designed to enhance the total operating effectiveness of the computer system. Multiprogramming and the advent of complex data bases would not be possible without this powerful addition to our technological repertoire.

Unfortunately, as the human interface relinquishes more and more control to the operating system, we are becoming increasingly dependent on the integrity and reliability of the system. Flaws or "holes" in the operating system which allow unauthorized individuals to access personal, proprietary or critical information (either accidentally or intentionally) must be eliminated, otherwise this situation could lead to a reduction in the automation or consolidation of a number of feasible but highly sensitive applications because users are unwilling to take a chance — witness the controversy over shared versus dedicated systems for criminal justice information.

But in a positive sense, software security provides the information-system executive with an important piece to the security puzzle. Considering the prodigious volumes of information that computer systems are capable of processing, the access control and auditing capability that a properly designed software security system can provide cannot be duplicated efficiently by any other combination of administrative and technological safeguards. In short, software security provides a uniquely efficient and viable security safeguard. It is the responsibility of the users to develop and enforce the administrative procedures and controls required to give substance to this technology.

Purpose
This section is intended to:

- Define the security requirements of operating systems, and
- Describe a possible framework of considerations that may be used to evaluate alternative software security systems.

Specifically, this goal will be accomplished by considering the following set of questions:

- What is a software security system:
- What are the desirable characteristics of a software security system?
- Does your data processing organization require software security?
- What criteria should be used to evaluate a software security system?
- How do you compare software security systems?
- What precautions should be taken to avoid problems in the implementation of a software security system?

What is a Software Security System?

For purposes of this discussion, a software security system is defined as a computer operating system certified as incorporating those hardware and software functions and features that are necessary to provide an accidental or intentional threat protection capability appropriate for the value of the information and resources managed by the system.

The software and hardware functions that will be defined in subsequent pages should ultimately become an integral part of future operating systems.

The Concept of a Software Security System*

The concept of the software security system (SSS) as a threat protection mechanism includes five fundamental characteristics:

- Integrity
- Isolation
- Controlled Access
- Identification
- Surveillance

The selection of these characteristics places additional requirements on the design of computer operating system software. Along with the conventional notions of accuracy, reliability, and efficiency, operating system designers are faced with the requirement to incorporate facilities for the **prevention** and **detection** of threats to the security and integrity of the organization's information.

Prevention involves the structuring of the system so that security goals are met.

Detection is the active determination of whether the prevention mechanisms have been circumvented, nullified, or destroyed by system penetration attempts.

The inclusion of these characteristics at the most fundamental level in the SSS architecture distinguishes the SSS from existing operating systems. An analysis of these characteristics and the reasons why their inclusion contributes to the protection goals of the SSS, requires consideration of the following set of questions:

- What are the principles comprising each characteristic?
- What are the potential adverse consequences incurred if the characteristic is absent?
- How should the characteristic be incorporated into the SSS as a specific function or set of functions?

The characteristics of software security contributing to the goal of threat **prevention** are: Integrity, Isolation, Controlled Access, and Identification.

*The software security system definitions contained herein were developed in conjunction with TRW, Inc.

• Integrity — The SSS must perform as certified.

Certification is defined as compliance of an operating system with a set or subset of designated specifications and/or standards to meet the requirements of a specific operating installation. As an element of software security, integrity is essentially the guarantee that the system is functionally correct and complete. It is compliancy with this guarantee that forms the basis for development of SSS certification criteria. The absence of integrity precipitates concern over the ability to guarantee protection by way of any of the other elements of software security. This is certainly true if the mechanisms which implement them cannot be relied upon. Thus, with its threat prevention and detection capabilities jeopardized, the SSS would fail in its role as a viable threat protection capability.

Integrity is not incorporated in a SSS through the addition of specific program modules, but rather is integrated within the structure of all operating system code.

• Isolation — Is the property of an operating system which insures the containment of users, information, and resources within the system in order to keep users separated from each other and from the protection controls of the operating system.

This concept acknowledges the increased resource sharing that is inherent in today's computer system environment. The ability to multiplex the processing of many different users requires the separation of each individual's data and status for reliable and predictable performance. Some specific examples illustrating the incorporation of isolation are:

Main storage access control (Fetch/store protection).
Privileged states and instruction sets (problem/supervisor state).
High level languages which isolate programmers from certain aspects of the machine (isolation by context).

Without isolation, confidential data would be exposed to compromise at various points in job processing. This type of exposure is greatest while the data resides either within main storage or within working data sets on peripheral storage.

• Controlled Access — Requires that each properly identified user is permitted a certain access to information and resources within the system to which he is authorized, but to no more.

A necessary provision for data security and integrity is the ability to control who has what type of access to the data and when. The protection of personal, proprietary and critical information in a large remotely accessed computer environment cannot be guaranteed without some type of enforcement mechanism established within the operating system software. The capability to define system resources (data sets, records, fields, programs, terminals, transactions, volumes, etc.) and restrict their accessibility (read, write, append, allocate, rename, scratch, execute, etc.) to authorized users on the basis of security levels, access categories, access periods, and a need-to-know, constitutes the concept of controlled access.

• Identification — The protection characteristic which assures that unique, machine readable names are assigned and authenticated for all defined users and controlled resources.

Isolation and controlled access provisions of the SSS demand the unique and authenticated identification of resources and users. The protection of resources and data from accidental or intentional disclosure or modification requires distinguishing between those users to which access should be permitted and those to which it should be denied. Identification schemes make it possible for the SSS to make this distinction. In addition, preventing intrusion by masquerading as a known user requires authentication of the claimed identity.

Conventional techniques for authentication of a users identity include special passwords or codewords associated with each permissible user name. Procedures common to remote terminal networks include "handshaking" protocols whereby users at both ends of the line periodically verify the identity of each other with a predetermined dialogue. It is an essential characteristic that the SSS include facilities for the consistent and authenticated identification of its users and resources.

• Surveillance is the characteristic of software security contributing to the goal of threat **detection**; specifically, it involves:

Detection of security related events (system behavior which constitutes or precipitates security incidents or attempted violations),

Collection, recording, reduction, and analysis of data regarding the above detections in order to invoke a procedure to compensate for or remedy the attempted security violations, and
Generation of reports for security personnel review and, if possible, damage assessment.

The principle of surveillance acknowledges the probability that threat prevention measures as incorporated into the SSS will eventually be subverted either intentionally or accidentally. This may result from a design or procedural "breakdown" and not necessarily because of any malicious intent. The fact remains that a quick, reliable, and consistent reaction is required to minimize any potential adverse impact. Some specific capabilities supporting the surveillance of a software security system would include:

Security audit log
Real time detection and administration and attempted security violations
Facilities for the certification and auditing of software security system integrity.

It should be noted that although surveillance is primarily a detection characteristic, the mere existence of this capability should serve as a psychological deterrent to the potential intruder.

Does Your Data Processing Organization Require Software Security?

It has already been noted that the operating system software is uniquely capable of authorizing access to the large number of resources within a computer system. In addition, its capability of acting as an automated, real-time security monitor cannot economically be duplicated manually. However, the decision to use software security depends on answers to the following questions:

- What is the cost and effectiveness of the software security system as a function of the kinds of logging and security options required?
- Will software security help your organization satisfy its legal and social obligations?
- Do your other administrative and technological safeguards afford the organization sufficient protection?

The answer to questions two and three lie outside the realm of technology, and should be addressed by management in general including the data processing executive. The first question on the other hand, requires the investigation of software security systems. The following pages should aid the data processing manager by describing the considerations involved in evaluating these systems.

What Criteria Should be Used to Evaluate a Software Security System?

A software security system may be evaluated from two viewpoints. Its capabilities may be compared with an operating system not containing many safeguards (the traditional operating system), or with another software security system. As a result, the comparison must be feasible through a wide range of protection capabilities. The data processing manager reviewing this section should focus attention on his particular situation by relating the material presented to his current operating system versus the software security system(s) being considered. If more than one software security system is under consideration, the problem of evaluation is twofold; he must now also compare software security system versus software security system.

It is convenient to analyze the requirements of a software security system within a framework of Evaluation Criteria. These criteria should provide a practical tool for data processing managers who may want to evaluate alternative software security systems. These criteria should also provide guidelines for manufacturers interested in user requirements.

For the purpose of this discussion, eleven criteria have been identified:

(1) Performance
(2) Maintainability
(3) Administrative Procedural Support Required
(4) Impact on User Application
(5) Impact on Operating Systems and Subsystems
(6) Ease of Implementation
(7) Ease of Use
(8) Functional Capabilities
(9) Flexibility
(10) Education Requirements
(11) Cost Considerations

The following pages describe some of the considerations and requirements comprising each criterion.

- Performance

The impact of software security on system performance is a legitimate concern. The installation striving to meet the processing demands of its users must weigh the value of software protection features against the anticipated impact on existing levels of service. The ability to identify and measure the impact of software security features on existing performance levels is paramount to its acceptance. What then are your major areas of concern related to evaluating the performance impact of software security systems?

Most software performance concerns can be found to fall into one of the following categories:

Functional certification
Software reliability
System degradation

Functional certification is the assurance that the software will perform its intended function.

It stands to reason that the absence of logically correct software is itself a potential threat to the integrity of the protection mechanism. After all, how much protection do defective seat belts and brakes provide a passenger riding in an automobile? The complexity of computer operating system software today makes it difficult to achieve 100% logical correctness, but the inclusion of security safeguards as a major design objective amplifies the requirement for this kind of accuracy. A fair measure of the software system's functional completeness can be determined from:

Reviewing the amount of maintenance activity reported to date by installations using the same software.
Functional Benchmarks of specific security features.
The eventual use of automated certification packages (though the state of the art still requires additional research and development).

Software reliability is the probability that the software will perform its intended functions for a specified time interval under stated conditions. If the software system does not perform consistently and without failure, throughput can be seriously reduced. How does software security improve reliability?

Software designed with the goal of preserving its own integrity at all times will make a positive contribution to more reliable levels of performance.

Controlled access of critical operating system resources from unauthorized or excessive use will reduce the possibilities of accidental or intentional failure.

Isolation techniques used within the architecture of the operating system will introduce a degree of "soft failure" as opposed to just "dying" when failures do occur.

Real-time surveillance by the software of its own status should detect penetration of system integrity before excessive damage can be done.

Other factors can contribute to a software system's lack of reliability. The interchangeable building block approach of system software needed for widely varying installation requirements introduces a high probability of potential human error. The installation and operation of complex computer operating system software today requires a high level of project control and systems assurance. The reliability of such systems is a product of many activities, including:

Functional certification
Sufficient education and training
Adequate documentation
Proper planning
Thorough testing
Controlled implementation
Detailed operating standards and procedures
Accurate and timely maintenance

Controlling access to critical data sets produces a concentration of responsibility for software systems maintenance. Controlled access requires the identification and classification of each data set including its content and use. Controlled access and data set identification results in better documentation of the system and contributes to a wider level of understanding.

Another source of poor software system reliability is inaccurate maintenance. A centralized maintenance activity and change control enforced by controlled access provisions of the software in addition to administrative standards can improve the quality of maintenance and thus the reliability of the software system's performance.

Two statistical indicators are helpful to management in determining the level of software system reliability being achieved and in establishing standards of reliability for an installation:

$$\text{Mean Time Between Failure (MTBF)} = \frac{\text{Elapsed Time of System Availability}}{\text{Number of Software Failures}}$$

$$\text{Mean Time Between Recovery (MTBR)} = \frac{\text{Accumulated Downtime Between System Failure and System Start}}{\text{Number of Software Failures}}$$

Objective analysis of software reliability data from other installations can be a helpful tool in evaluating software security performance. Recognize, however, that reliability is a function of human and installation — related factors as well as the design of the software system. Therefore, caution should be used in comparing MTBF and MTBR of one installation with another. These indicators may be more helpful in comparing software systems within an installation and in tracking the ongoing performance on an installed system.

Software systems can generally be expected to prove more reliable than their counterparts of the past decade. Historically, performance has been far below even a resonable expectation, but recently there have been predictions indicating a turn for the better. Asone IBM spokesman speculated:

> *The programmer of the next generation will not only produce less than one error per year, but he will also remember every error that he has made during his career.*
>
> *IEEE Symposium*, DATAMATION,
> Volume 19, Number 10, pg. 119, October, 1973.

Estimates of *one error per 10,000 lines of code* are not out of bounds considering the potential impact of software security effectiveness.

System degradation is a measure of adverse operating performance as compared to some previously achieved installation standard. Adverse operating performance is manifested by the decrease in job turnaround time, system throughput and teleprocessing response times. It appears logical to surmise that an SSS which performs more functions than the installation's current system inherently uses more system resources per unit of user tasks processed. The amount of extra resources required produces a degree of system degradation. The level of degradation is either directly or indirectly dependent on the system design. In some instances it may be possible through a system specification analysis to determine that one system will perform more efficiently than another — but this is usually not enough. Quantitative estimates must be obtained from one or more of four possible sources:

(1) Performance Records — Other installations using the software security system may have performance data available based on actual production experience.

(2) Benchmarking — By taking a well-defined production jobstream (benchmark jobstream) to a similarly configured data center operating the software security system, performance data can be gathered.

(3) Vendor estimates — The software security system vendor should provide estimates of increased resource utilization (CPU, I/O components) for various software security functions (e.g., authorization and data sanitization).

(4) Delphi Technique Estimates — This technique, as described in Appendix D, may be used to estimate levels of degradation through a poll of knowledgeable individuals.

After estimating the system degradation of a particular SSS, the installation should determine if its impact falls within acceptable boundaries relative to the security service provided. If so, another concern remains — isolation of the impact. Specifically:

What points in the processing cycle does degradation impact?

Does degradation occur as system overhead?

Is degradation absorbed by all user jobs to be subsequently paid for by all users?

Is degradation absorbed by only those user jobs requiring security services?

The answers to these questions may be obtained from a performance study utilizing hardware or software monitor tools. Hopefully, the need for such a user study can be avoided through appropriate SSS vendor documentation addressing these issues.

Impact should be felt by only those users requiring specific security services. The ideal SSS should have accounting routines which monitor security function usage based on the requesting task. These routines would then store descriptive information so that the installation's billing algorithm could include security charges. Those services which are not specific should be accounted for as system overhead. Consider, for example, system integrity and isolation functions. These are functions which every user should expect to be part of the service offered by the operating system. In fact, many of your organization's users would probably be surprised to find that they do not have this protection now!

A study was conducted by the Project to determine the extent of system degradation caused by a prototype SSS. Future systems should have improved performance based on some of the findings. The environment, techniques used, and results of this study are included as Appendix E.

- Maintainability

The support of computer operating system software today is a large scale operation requiring a major commitment of resources by your organization. The nature of such support involves a cycle of activities, including:

Planning
Education
Generation
Implementation
Operation
Maintenance

The ability to provide and maintain adequate support in each of these areas is important and generally affects the overall effectiveness of the computer operation. You must be concerned with factors that could influence the maintainability of a software security system and thus impact the effectiveness of your computer operations.

The support of today's software systems is typically a combined effort on the part of both vendor and inhouse personnel. The size and complexity of the system usually dictates this requirement. Therefore, the impact of software security on both of these groups must be considered.

Three basic concerns of the maintainability of software security exists. They are:

Changes in the amount and type of support required

Upholding maintenance integrity

Impact on software support productivity and activity

The information systems executive responsible for budgeting, staffing, and education of the software support function must be concerned with any change in the amount and type of support required to maintain the software security system. Some appropriate questions that can be used to assess your situation are:

Will there be an increase in the amount of support required with the software security system?

Will such an increase affect in-house staffing levels? Vendor staffing levels:

Will an increase in the amount of required support affect in-house staffing levels? Vendor staffing levels?

Must additional vendor related support be located at your installation?

Will there be a change in the degree or type of support or expertise required for the software security system?

The major provisions of software security should not drastically alter the activities of people currently engaged in the support function. Software security, as with any new feature of the operating system, must be supported and included in all plans surrounding the reconfiguration of the system unless you are willing to risk rendering security provisions impotent.

The realization that the software will occasionally fail (because of design flaws, programing errors, etc.) requires the development of a mechanism for the accurate and expedient application of fixes to the system. You should be concerned with the impact of software security provisions on the ability to perform maintenance on the system. Also, you must consider the impact of maintenance on the integrity of the security features. Consider the following questions relating to maintenance integrity of the software security systems:

Will problem reporting/resolution procedures be affected?

Do problems dealing with security functions require special handling?

Do specific maintenance tools generate security exposures?

Careful consideration should be given to the existing user/vendor problem reporting/resolution procedures. Consider the impact of publicizing a known problem with a security feature to all users of the system. No installation would want the outright advertisement of a security "loophole", particularly within the service bureau environment with many users at remote terminals. The awareness of a "loophole" at one installation would also represent an exposure to another. Tighter controls over who receives information of this type will be required to minimize the potential adverse consequences.

Also consider the exposure in the Program Temporary Fix (PTF) transmission procedures.

Are you sure the PTF has been delivered from the correct vendor source point?

Has the PTF been susceptible to interception and/or modification enroute to your installation?

Who receives the PTF at your installation?

Current transmission procedures must be modified in order to maintain the intergrity of PTFs.

Once the solution to a problem is known, the application of the fix itself may be a problem. Assuming security features are somehow certified as correct upon initial installation of the system:

What procedures should be established for their recertification after a fix has been applied?

With the high amount of maintenance being performed on present software systems, is it practical to expect recertification after every fix?

Certification of software security system maintenance activity clearly requires each installation to evaluate for itself the advantages and disadvantages of such a process. Some of the variables involved in this analysis are: the certification tools available; the amount of maintenance activity; the induced *slow down* of the support function; and the degree of risks involved (e.g., the integrity of personnel assigned to the application of fixes.)

The adoption of software security system provisions in general will have a sobering effect on the software maintenance support function. The overhead required to control critical system data sets will be felt by support personnel and initially, at least, resented by them. The assignment of access rights by type will have the effect of controlling their activities. Access capabilities that heretofore have been unrestrained and unchecked will be assigned on a "need-to know" basis only.

While it is not the purpose of software security systems to impede the progress of the support function, the controlling influence does have the potential for introducing both psychological and operational bottlenecks. The system programmer who wants to allocate a new system data set requiring protection, does not enjoy being inconvenienced by authorization procedures. Changing the behavior and attitudes of all personnel affected by the software security system is the key to its success. The motivation of software support personnel to work **with** the software security system rather than **against** it will be a primary factor affecting its maintainability. An adequate education program is crucial in establishing this motivation.

Up until this point, system access considerations have applied to all maintenance personnel in general; however,

What specific requirements exist to assure effective, yet controlled vendor support?

The Programming Systems Representative (PSR) must have access to those libraries containing the vendor diagnostic aids. Special considerations exist if a diagnostic aid is available which allows the on-site PSR to form a CPU to CPU hookup for remotely-based component specialist assistance:

There may be no assurance that data required for debugging will not be removed from the remote location. (Data removal can be controlled at the local site by physical security measures such as locked doors and guards.)

In a CPU to CPU environment, what check will be made on the remote CPU? Will the local vendor employee connect to the remote support CPU, or will contact be made with a CPU at another location for the purpose of obtaining sensitive user data?

The SSS will inhibit hardware maintenance personnel from executing their assigned functions unless plans are made to allow access to system hardware components. These personnel must be given access to not only defined system resources such as terminals or printers, but also to the vendor diagnostic libraries. This situation is crucial because it has a potential impact on system "down time".

- Administrative Procedural Support

Administrative support, particularly procedural change or development, is required to successfully install and operate a software security system. In many cases, new or changed installation procedures are not merely a desirable complement to the system, they are necessary to accomplish the overall goal of installation security. Therefore, the degree or level of administrative procedural support required should be considered when evaluating the capabilities of a software security system.

Procedural requirements will vary between systems and also within a given system depending on the specific functions used. Ideally, the system will require minimum procedural support through well-defined and easily used "man/security" interfaces.

What kinds of procedures must be developed to implement and operate a software security system? Examples include procedures for:

Gathering user resource protection requirements
Disseminating user passwords
Auditing the software security system
Accessing system libraries for updating capabilities
Handling attempted violations of security
Handling specially labeled output
Backing up confidential or critical data
Operating the installation on off shifts (second, third, holidays)
Authorizing system access to vendor, hardware, software and maintenance personnel.

This list, although not exhaustive, should provide a guide for the type of procedures required. While it may be difficult to determine the complexity and level of support required for substantive procedures, the experience of other installations should provide a helpful reference.

Project SAFE has found it desirable to incorporate the software system related procedures and responsibilities into a single manual (*Recommended Security Practices*) which includes all procedures necessary to achieve a secured automated facility. Most of these procedures have been tested successfully at the Management Information Division. This document should serve as a useful reference.

- Impact on User Applications

For the most part, a SSS should be transparent to the user and his applications. However, since few existing applications have been designed/coded with security in mind, problems will undoubtedly surface during conversion. Although subtle inconsistencies may unexpectedly arise, the areas most probably impacted include:

Integrity
Job Control Language
Field/Record Level Security
Volume Control

Integrity — Integrity problems generally may be avoided by following coding standards recommended in the operating system documentation. Problems arise when a programmer attempts to short-cut system-provided user functions or to execute a function that was designed to be used solely by the operating system (e.g., modification of system control blocks, attempting to run as a system task, execution of privileged operations or macro instructions, etc.)

The number of integrity problems that an installation can expect to encounter during installation of a SSS is directly proportional to the number of integrity "fixes" in that system. The vendor should supply a list of newly protected areas. An analysis of this list considering the functions required by your applications, should reveal the areas of greatest potential impact. Unfortunately, in many cases the existence of a new problem depends on the coding method used and cannot be detected by reviewing the application design documentation. Paradoxically, the more intelligent and ingenious the programmer, the more likely generated code will contain some type of integrity violation. Since most integrity problems cannot be predicted, the DP manager should compare the number of integrity "fixes" in the SSS with the software functions required by a given application and the degree of system "savvy" acquired by his application programmers.

Job Control Language — Although the SSS will perform most of its functions automatically, the user may be given the option to make specific requests within his job control language. These requests will be made through the addition of new parameters or key words within the language. An example of a potential request might be the capability to perform a sanitization operation upon data set deletion. Another language consideration is the likelihood that it will contain a job identification capability such as a password. Any additional language requirement can be previously identified by scanning the list of new parameters/keywords in the SSS documentation.

Field/Record Level Security — To take advantage of a field/record level security capability within a SSS, the application must satisfy certain requirements:

It must contain a data dictionary definition technique in accessing data within files. Thus, **every** access to a logical block of data is made through the usage of a pre-defined name or key.

The application must contain an interface to the security mechanism to perform authorization.

It must have the ability to terminate requests causing field/record level violations and record the event.

Design incompatabilities between the SSS and programs may prevent an application from immediately taking advantage of the SSS interface without a coding change.

Volume Control — Since the SSS may provide a volume definition capability, the user is subject to specific problems if one of his volumes is either lost, damaged or encounters permanent I/O errors. While it may be necessary to replace the volume, the user may not have the option to simply use a temporary volume through an appropriate job control deck change. This SSS restriction requires that the temporary volume be previously defined before the job is run to avoid bypassing data set control. The user must, therefore, plan for events of this nature by either:

Establishing procedures with Security Office personnel to effect immediate definition procedures, or by

Previously establishing a pool of volumes to be used during such emergencies.

Other impacts — These will vary from system to system and should be documented in the proper manuals. Some areas of potential concern include:

Bypass Label Processing (BLP) cannot be used freely if volume *access* control is necessary.

Volume **contamination** control allows both permanent and temporary data set allocation to occur on designated volumes only. The volumes must be designated in advance through criteria established by installation management. Control is maintained through profile definitions.

Utility functions available with current operating systems may be somewhat limited in the SSS in order to preserve security.

Macro statements may be available which the programmer can use within his programs (e.g., header/classification labeling technique for program output).

All user restrictions and selective capabilities within the SSS should be documented by the vendor in a consolidated manner (e.g., an SSS user's guide). You should evaluate the design of existing and future applications in light of this documentation.

- Impact on Operating System and Sub-systems

A software security system (SSS) should be capable of being installed with many different functions. The functions selected will determine the extent to which software security will impact an operating system and its sub-systems. The selection of these functions will be determined by the need of a particular environment.

Specifically, the considerations involved include:

Patched-in security versus security as an integral part of the operating system.

Control of utility functions.

Consistency and compatibility with sub-systems.

Patched-in Versus Integral Security — The integrated SSS has security concepts designed into the operating system from its inception. In this type of system, most of the security functions operate as an integral and logically extended part of the operating system.

A patched-in software security system is one in which security functions have been added after the system design specifications have been finalized with the intent of plugging known exposures or adding security function. In this type of system, many of the security functions operate as tasks separate from the operating system itself.

The most serious flaw in a patched-in system is that the security function is not being handled by a logical system task but rather through a convenience mechanism. For example, the system is first analyzed to determine at what point a security check might be added. This decision is based on the design of the original operating system which never made a provision for the insertion. The disadvantages associated with this type of approach range from increased overhead to illogical processing flow. This general technique through its very nature is prone to both anticipated and unanticipated exposures.

In analyzing the inherent differences between a patched-in security system and an integral security system, you must also be concerned with:

How difficult would it be to support an SSS as an operating system extension as compared to an integral part of the operating system?

This point should be addressed in terms of installation time, support and maintainability. A patched-in security feature would require post system generation installation rather than automatic inclusion at SYSGEN time. Support and maintainability should be simpler in the integrated system. Why is this the case? Suppose a problem occurs within a patched-in system which the user cannot isolate, but the problem appears to be due to security code. This situation is quite possible since security functions are executed throughout the operating system's processing. To whom does

he send the problem report? Even if the same vendor has supplied both the operating system and the security functions, additional time may be consumed in determining which internal maintenance group should resolve the problem.

Are there significant overhead differences between the two types of systems?

Again, installation time, support and maintainability are important factors in determining the cost differences, but the key factor should be system degradation. Most patch-in security systems will generate additional load modules. The overhead involved in transfer of control to such additional modules must be considered.

Software security functions should most definitely be an integral part of the operating system. As noted by Anderson in a *Computer Security Technology Planning Study* for the Air Force:

> *The issue of computer security is one of completeness rather than degree, and a complete system will provide all of the controls necessary for a mixture of all security levels on a single system. It is the notion of completeness that compels one to take the position that security must be designed into systems at their inception . . . Unless security is designed into a system from its inception, there is little chance that it can be made secure by retrofit.*

Utility Functions — The utilities supplied by the operating system are vital to the users of that operating system. Certain restrictions should be imposed on user type utilities, however, to maintain the integrity of the security system. They should not be allowed to function any differently than that of a user written program. By applying this restriction, the users will be able to use the utility functions in their problem programs without possibly violating security. Utilities that can be used to circumvent security safeguards should be maintained as system utilities with limited accessability.

Sub-systems — Sub-systems should be provided with the same levels of security as that incorporated into the operating system which controls batch job processing. This means that the five fundamental SSS characteristics should apply to sub-system design as well. Such a provision allows for consistency and compatability throughout the entire complex system.

Just as important as providing functional capability is the quality of providing standard interfaces wherever possible. Thus, various sub-systems will interface using an identical set of specifications. This interface could be provided through the use of macros, supervisor calls (SVCs) or a front-end processor to invoke the security functions.

Sub-system software should be easily modifiable with minimal changes, to avoid altering or degrading the intended function of the sub-system. To maintain a high standard of reliability in sub-systems, you must avoid making detailed changes to *mainline* code in an attempt to support the security function. This is *not* to say that sub-system vendors should anticipate specific security functions, but to ensure that sub-systems are modular in design to enhance adaptability to the security system.

The standard interfaces will be used to transport security related data from the sub-systems to the security function and back again. Thus, both the operating system security function and the sub-system are performing security related tasks. To maintain consistency throughout the system, it is important that the sub-systems perform a minimal degree of security. Therefore, the sub-systems should primarily be responsible for:

Gathering sufficient information surrounding requested resource usage and user identification, and

Assisting the SSS in handling attempted violations.

Each sub-system must accommodate these requirements according to individual installation security needs. A discussion of detailed considerations pertaining to some specific sub-systems follows.

Remote Job Entry (RJE) Systems — RJE poses special problems in the attempt to maintain security.

Is there an adequate procedure to identify/authenticate the RJE user?

Should this procedure be periodically repeated or executed only upon initial sign-on?

How should attempted sign-on violations be handled?

How should attempted violations during job execution be handled? (Possibilities include disabling the terminal, withholding job output, delaying notification to user of job status, etc.)

Is job routing over RJE lines strictly controlled?

You should be aware of the capabilities of the SSS and how they match your RJE requirements. You should decide for your particular environment, what restrictions should be enforced in order to maintain security.

Teleprocessing (TP) — A teleprocessing system is a collection of terminals that use communication lines to access the facilities of the computer through the use of pre-programmed transaction This type of system is prone to users tampering with the system in an attempt to break its security. Isolation is a primary problem in a TP system, because the distance factor involved makes it very difficult to control the user of a terminal. In order to physically control the activities of TP system users, you must have tight controls over access to the system. When evaluating the protection capabilities of a TP system, you should answer the following questions:

How is identification and authentication handled for users of a TP network? Are the procedures adequate for your system?

Can defined terminal accesses be restricted to time-of-day?

Should defined terminals be automatically signed-off after an extended period of inactivity?

In cases of attempted violations, can the network always identify the responsible terminal/user?

How should attempted sign-on violations be handled?

How should attempted processing violations be handled?

How effectively does the TP sub-system restrict TP user capabilities through high level language (isolation by context)?

Is selective terminal buffer sanitization a capability?

In the event certain hardcopy terminals do not provide a print inhibit feature, does the TP network overwrite user accounting/codeword information?

Timesharing Systems (TSS) — A timesharing system (TSS) differs from a TP system in that a terminal on a timesharing system is capable of programming and executing a variety of programs under the control of a single sign-on. Timesharing systems typically offer a wide range of extensive capabilities and thus present a great potential threat to data and system security.

All of the considerations mentioned in the TP section also apply to the TSS. There are two additional primary areas of concern, however:

The increased flexibility of the command language over the preprogrammed transactions of the TP system — does the TSS access the SSS interfaces within the various TSS commands?

Swapping of main storage among TSS users — does the TSS sanitize main storage prior to access by a subsequent user? Are user main storage boundaries observed within the TSS region?

Data Base Systems — In an attempt to eliminate redundant data, file consolidation has become a common practice throughout computer information system applications. Because of this increased sharing, integrated data base and file management systems need the capability to control multiple users of the same information. This control potentially can involve three levels of security:

File Security
Record Security
Field Security

In order to provide the necessary detailed level of control over an integrated data base, the subsystem must perform certain functions:

It must use a data dictionary
It must allow access only through dictionary terms
It should handle attempted violations in a manner suitable to the installation.

This detailed level of control will probably induce a high degree of overhead. It is mandatory that techniques be developed to minimize this overhead.

- Ease of Implementation

The SSS must be designed with implementation considerations in mind. To evaluate the SSS, you must consider the following questions:

What does the SSS include that will ease the implementation for the following groups in your organization?

Management
Security Office
Software Staff
Operations Staff
Users

What support will the SSS vendor technicians provide to ease the implementation?

A well designed SSS should possess the following characteristics which will assure the smoothest conversion possible for the following groups in the organization:

Management — The SSS vendor should provide management with an overview of the information required for planning the conversion, installation and operation of the SSS. This documentation should include data concerning the degradation caused by the additional functions of the SSS and the estimated manpower requirements to install and operate the SSS.

Security Office — Presently, most security offices are concerned only with physical security. The advent of the SSS means additional responsibilities will be required of the security office. The security office will now be involved with the organization's computer and data files. Of particular concern, is the initial establishment of the security profile. To enable the security office to perform these new tasks, the vendor must provide complete documentation on the functions of the SSS and their use. Since this information is new to the security office staff, the vendor must provide the required information in a precise and complete fashion.

Software Staff — The software staff will require complete information on the SSS which explains:

How to select required security options.

The system generation process.

How to plan and allocate space for the profile data sets.

How to plan and allocate space for the audit trail data sets.

What changes, if any, must be made to catalogued procedures.

What changes must be made to the standard region size or other system parameters.

How to tune the SSS to perform efficiently.

Problem determination aids to decrease problem resolution time.

In addition to documentation, the software staff will require exits that can be used for local modifications such as accounting routines and librarian systems. These exits must be well defined and controlled to avoid potential compromises of system security.

Operations Staff — The operations staff must have documentation which supplies the following information:

What hardware support is required by the SSS?

What configuration changes are necessary due to additional data sets or space utilization?

What amount of test and conversion computer time will be required?

Users — For the users of the SSS, several items could be provided that would ease the burden of implementation. For example, preprocessors and temporary bypasses.

A preprocessor which would scan the installation's programs or JCL before attempting to run test or production could prove to be an invaluable tool to find conflicts between the programs, JCL and the SSS. The JCL scan could also be used to aid in the definition and use of resources.

Bypasses could serve as a replacement for preprocessors in the SSS. These bypasses, which allow the SSS to log the conflicts but not terminate the running job, would not be as desirable as a preprocessor because users will tend to ignore the problems in lieu of correcting them.

If, however, the SSS does not provide either preprocessors or bypasses, two computer systems may be required for the conversion to the SSS. The SSS could then be installed on the first system with the other used for unconverted jobs or for jobs within which conflicts appear after entering production on the SSS. Once the SSS enters production on both machines, there will be no bypasses for unconverted jobs. This will tend to force the users to "clean up" their application systems.

To answer the second question, you must first evaluate your present installation. If you presently require vendor support, at least the same amount of support will be required for the SSS. If your installation presently requires little vendor support, other than education, no additional operational support should be required. However, some vendor support during the planning and implementation phases could prove invaluable.

The SSS should not prove to be more difficult to implement than any other operating system. It will take longer, however, due to the extra functions that will be implemented.

- Ease of Use

The implementation of a software security system provides the installation with its initial exposure to the operation and working concepts of software security techniques. An important factor in analyzing systems is determining how these concepts have been designed from the standpoint of ease-of-use. This criterion should be of even greater importance than ease-of-implementation since security use and maintenance is an on-going effort affecting the entire installation. The DP manager should be aware of the types of system functions which he can investigate from a usability standpoint. This can be done by considering the installation organizational interfaces to the system.

Security Office — The Security Office has the responsibility for maintaining system security at the level prescribed by management. The software security system will provide this office with facilities to achieve this goal. Are these facilities easy to use?

One necessary capability is that of real-time access to the security profile(s). This access will most likely be given through a unique *command language* which has the ability to build, update and list the contents of the profile upon request. There are specific items with which one must be aware when determining the usability of such a language. This command language should:

Be syntactically consistent and as brief as possible.

Have a full as well as an abbreviated free form format (the full form should be self-descriptive and the abbreviated form should be used once the user becomes familiar with the language.)

Be capable of manipulating groups of user and resource definitions as well as individual item definitions.

Be capable of creating a "parent" group from several other groups.

Provide for items to be easily added to, deleted from or changed within groups without affecting the group or unrelated items within.

Allow the user installation to specify limits of quantity within the profile with no restrictions caused by SSS coding techniques.

Be capable of being entered from a terminal device as well as through a device which handles mass data (card reader, tape, etc.) In both cases, the commands should be identical in format.

Have a comprehensive reporting capability to display profile status upon request. This reporting capability should include installation "formatable" reports produced through easy-to-use format/macro statements.

Allow two or more terminal devices to concurrently access the profile.

Allow for the replacement of defined I/O volumes with ease (in case of permanent damage to original volumes).

These considerations relevant to command language usability are certainly not exhaustive.

Another usability issue is that of *profile update restrictions.* The ideal software security system should:

Allow unrestricted update and/or profile swapping during production processing. The action would be initiated at the discretion of the security office without adversely impacting the system. This particular feature allows changes to be applied immediately rather than causing a dependency based on production system availability.

Have the ability to move, swap, backup or restore profiles easily through a set of catalogued procedures and system tasks or through security commands. Security commands, if properly designed, would be the better approach from two standpoints; they would be an easy-to-use technique and they would eliminate the need to train the individual in JCL procedures.

Allow for the ability to increase the size of the security profile data set without altering its contents in the event that installation profile requirements change.

Other usability issues affecting the Security Office should:

Have the ability to transfer a profile from one CPU to another in order to maintain the active user codeword list.

Provide the capability to test new profiles for accuracy without having to run pseudo production jobs against the profile.

Provide descriptive diagnostic messages. Diagnostic messages fall into two broad categories; software security status messages and attempted violation notifications. The status messages pertain to system functioning. These messages should be categorized into such classifications as "information only", "warning" or "action required" with the message ID containing the classification type. The messages should contain complete and concise text.

The attempted violation notification diagnostics should contain all the data needed by the security office to determine who is the violator, the type of attempted violation and the resources involved. Other items may be helpful in tracing the violator; i.e., job name, date and time.

System-Programming Staff — System programmers, although comprising a small portion of the total data processing staff of an installation, require the most potentially damaging (software) authorizations. Whereas user production libraries are relatively static, system libraries are constantly being updated by fixes, additions or desired changes.

The SSS must be capable of allowing such necessary updates while maintaining as high a degree of protection as possible. An SSS must have an easy to use control mechanism. The degree of ease necessary should not be impacted by the degree of control desired.

Several alternative concepts should be considered to restrict the system programming staff's daily authorization requirements.

Alternative [*1*] All system programmers have authorization to updata all system libraries,

Alternative [*2*] Selected programmers are authorized to update selected libraries as owners and are responsible for these libraries,

Alternative [*3*] One programmer (or a small group) has authorization to update all system libraries,

Alternative [*4*] No one has daily authorization to update all or selected system libraries. Authorization is given on a temporary, "as required" basis.

These four concepts are characterized by the progressively increased tightening of control. As tightening increases, however, the impact upon the programming staff ideally should not increase beyond the restriction imposed by selective authorization itself. The programmers, for example, should have no increased requirements for job submittal (extra passwords, job control statements, programs). A minimal set of procedures should be required for system interface regardless of the access concept used.

Another area concerns the use of *security profile and core dumping aids*. These aids should be simple to use, yet provide all the information needed in a well formatted report so that debugging is easy.

To what degree does the nature of the system impact software testing? As the system programmers develop new programs for system interface, special needs will become evident. These programs may be intended to use, for example, priviledged operation codes, or be run as a system task or as a system user exit function, etc. Testing these types of programs may be more difficult under various software security systems. Does the SSS supply a special facility for this need?

Maintaining current backup copies of the installation's system libraries is one of the most critical jobs to be performed. Since many system libraries are located on a few volumes, the ability to dump/restore these volumes requires a "blanket coverage" of all data within. This situation requires a unique software capability for allowing a restricted type of access to the volume. Does this method impact current practices? Does it require additional procedures?

Another consideration centers around the work involved by the staff in the event the SSS must be temporarily backed out. One case in point involves user passwords. Once a software security system is in production and users have been using passwords in their jobs, backing out to a previous system in order to resolve a problem requires reversion to non-password jobs. To avoid this problem, the system programming staff could modify the non-security system to ignore the job password.

Perhaps the most difficult area to assess is that of determining the ease with which system, sub-system and application upgrading and maintenance can be performed. Some insight may be gained by investigating the SSS complexity of design or by the length of time it takes a system programmer to understand its internal processings.

Operations Staff — The additional functions provided by the SSS places increased demands on the operations staff. The degree of demand, however, can be minimized by considering three areas of interface:

Operations must handle a new set of system messages pertaining to various security functions — The SSS should have a functionally oriented message routing mechanism which limits only necessary security messages to operation consoles. Definite distinctions should be made for messages warranting routing to the Security Office. The types of messages that operations should be aware of are only those relating to the security task's interface with the system or functions affecting system resources (printers, memory, terminals, etc.), as opposed to attempted violation messages.

The handling of output generated by the system — Every type of output related to the security function should be identified by the data processing manager when evaluating a system. This output may be user generated with imprinted security classifications or handling techniques requiring operation staff procedures and routing paths beyond those already in existence. On the other hand, output may be security task related containing such data as profile printouts or security debugging aid reports. These require special handling also. The volume and types of system output will vary among software security systems. This has a direct impact on the number of operating procedures required.

The third area of concern applies to those installations in which operations has the responsibility for running certain jobs; i.e., accounting runs, backup/restore runs, certain library maintenance runs, etc. — In these cases, the selected operations personnel will be considered as system users and be required to have passwords. They will also be subject to any of the constraints that software security places on system users.

Users — From the users' standpoint, the SSS which is easiest to use is the one which is most transparent to him. He will be subjected to some constraints by any SSS, for example:

There will be a requirement for the user to identify himself in a job, and the system should provide a simple method to accomplish this.

Users may be more restricted in the system utility functions which can be used.

In order to build the security profile, the user may be required to furnish data to the security office. The amount of data necessary is dependent on the profile method used. It may also depend on the number of steps within jobs. A lengthy job passing controlled data from step to step within *permanent* data sets requires all these data sets to be controlled, not just the initial input and final output files.

The installation which presently condones testing of newly developed application programs with production data files may incur yet another impact. Since the personnel normally authorized to controlled production data sets are not the application programmers, the programmers will no longer have access to them. Thus the need for the creation of test data files for all confidential applications in the testing phase becomes mandatory.

The user should have a capability within the SSS to label output. This facility should be optional and easy to use, and should contain, if desirable, user requested:

security classifications on data separator pages

security classifications on the top and bottom of all data pages

x of y pagination.

Documentation provided with the SSS by its vendor should state all known user constraints so that non-transparencies may be resolved in advance.

Installation Staff Interactions — The degree of interface necessary between the security office, operations, systems programming and users will vary from one SSS to another. Interfaces require written procedures and consume personnel time. Fewer interfaces will be required if the system routes output directly to the appropriate individuals rather than to an intermediate point. (Hardware configuration plays a part here.) The degree of interface also depends on the level of centralized authorization to be maintained by the SSS. Authorization centralization will be discussed in the section on flexibility.

- Functional Capabilities

Software security systems, while subject to scrutiny on the basis of other qualities (e.g., performance, maintainability, etc.), must ultimately be evaluated on their functional capabilities.

The specific safeguards incorporated into the operating system exist to reinforce the conceptual characteristics of software security. It is by their inclusion that the software security system is able to provide a viable threat protection capability. As the data processing manager evaluating the functional capabilities of a software security system, you should ask the following questions:

Does the software security system contain those functional capabilities required by your organization?

How effective are the available functional capabilities?

To what extent do missing functional capabilities jeopardize achievement of the required level of software security?

The process of matching the organization's software security requirements with those functional capabilities that are provided within the software security system requires: (1) identification of exposures that exist as a result of the absence of software security provisions; and (2) identification of specific functional capabilities within the software security system which will eliminate the known exposures. You are responsible for the assessment of your organization's vulnerabilities and risks and it is by this action that specific requirements for software security should be outlined. Identification of software security system features which address these requirements and ultimately justify their inclusion is also your responsibility and will require some knowledge concerning what to look for in this area. The functional capabilities of a software security system should be evaluated in relationship to their specific contribution to the five fundamental characteristics of software protection:

Integrity
Isolation
Controlled Access
Identification
Surveillance

As a result of Project Safe's study and work with a prototype of future software security systems, a list of specific capabilities is presented to assist you and your staff with your analysis.

INTEGRITY

The capability to prevent all application programs and sub-systems from compromising the software security system integrity.

The capability to reconstruct security profiles in the event of I/O errors without having to IPL.

The capability to notify the security operator of other unusual conditions (e.g., capacity of profile reached) on the security profile without damaging or interrupting the system.

ISOLATION

The capability to allow for the de-centralization of security operator functions.

The capability to sanitize sections of a direct access storage or tape file after the data set is deleted.

The capability to control the placement of data on a direct access or tape volume.

The capability of protecting each user's programs and data, while resident in main storage, from both reading and writing by other users' programs.

The capability to fetch protect sensitive system data (i.e., security kernel).

The capability to determine what data is needed when a main storage dump is taken and give only that portion.

The capability to maintain a security audit journal separate from all other system logging facilities.

The capability to route security messages to specific security consoles.

The capability to sanitize the buffers on all I/O devices.

The capability to sanitize all freed main storage.

The capability to control which devices will be used for security output.

The capability to restrict the execution of system functions (e.g., privileged state) to specific programs.

IDENTIFICATION

The capability to uniquely define system resources and their characteristics to the security system.

The capability to uniquely identify and authenticate all users of the system.

The capability to provide randomly generated codewords (if codewords are to be used for identification).

The capability to allow the use of undefined resources both during and after the conversion to the software security system.

The capability to allow terminal-oriented sub-systems to use the identification provisions of the security system.

The capability to label printed output with a security classification, page numbers, date and time.

CONTROLLED ACCESS

The capability to prevent unauthorized attempts at signing onto the security operator console.

The capability to dump/restore complete disk volumes with authorization to the volume table of contents without authorization to the data sets that reside on that volume.

The capability to display the file identification from tape when serial number or data set name is not known. Bypassing file labels should not be permitted.

The capability to have different periods of access in order to authorize personnel to resources during working periods.

The capability to delete residual temporary data sets from work packs without being in a privileged state.

The capability to control which programs will be executed, added, or replaced by a user on the basis of his security level, access categories, and need-to-know.

The capability to restrict access to data sets, programs and terminals on the basis of hierarchical security levels.

The capability to control access to data sets, programs and terminals on the basis of a need-to-know or through access categories.

The capability to define and control access to individual fields of data by field name and security level.

The capability to control all system data sets (e.g., the system catalog) in the same manner as all user data sets.

SURVEILLANCE

The capability to include into a security audit journal the following:

any access to sensitive information,
any use of critical resources,
any changes to the access control profiles,
any unauthorized attempts to sign onto the security operators console,
any attempted security violation.

The capability to audit system integrity in either real-time or batch mode.

Effective software security requires effective functional capabilities. The feature that is included with security "loopholes" will diminish the threat protection goals of a software security system. A case in point is the software security system requirement for a security audit log.

While sound in concept, the manner in which the security audit mechanism is implemented is a measure of its effectiveness. The sensitive nature of security log data requires recording it separately from normal accounting data. A software security system that does not acknowledge this need would impact the control of such data and reduce the overall effectiveness of such a feature.

The overall value of a software security system will ultimately be determined by its ability to satisfy your requirements for software protection. The presence of effective functional capabilities to give substance to this protection is important and should be used by the data processing manager to evaluate its worth.

- Flexibility

An important evaluation criterion in a software security system is the degree of flexibility incorporated into its design. Each installation has distinct software security needs and should be given the ability to employ a system in which the security functions exactly match those needs. Cost/benefits of software security flexibility include savings in machine/system overhead and reduced training costs.

Two aspects of flexibility need to be considered; flexibility in implementation and flexibility during use:

Implementation flexibility includes being able to select only those functions required by the installation from among a range of software options. Only necessary functions are included in the SYSGEN — saving the code and operating overhead associated with the functions not selected. This means that the installation requirements must be understood in advance.

Flexibility during use involves being able to change the security functions in use as the needs of the installation change. This change could be accomplished by a "security only" SYSGEN through special macro statements applying only to the security functions that need to be changed. In a modularly designed software system, the changes would be simple to accommodate.

What types of functions, then, should the installation be able to include or omit depending on individual needs?

Profile Report Formatting — Through a set of format macros, various desired profile reporting programs will be automatically built and included in the system. These reports are used by the security office to examine profile status.

Security Accounting Routines — In order to provide the capability to charge users of security functions for specific security requests, programs may be included in the SYSGEN which monitor security functions. They would be a logical extension of the operating system's regular accounting scheme. Such items as main and device storage sanitization (which should be capable of being performed upon request) and profile access by job may be monitored. An installation should be able to select only those functions it wishes to monitor based on the chargeback algorithm in effect.

Certification Routines — Various levels of certification or threat monitoring routines should be capable of being individually selected. These routines would be activated periodically based on some condition such as a timer interrupt. They would provide various system checks automatically; e.g., scan system control blocks for inaccuracies, make storage checks, issue violation attempts, test the profile for unfavorable conditions.

Audit Trail — Different degrees of recording in the security audit trail should be available. This trail, which provides a history of resource access by type, should be capable of recording any information as determined by the installation. Thus, the installation can determine, based on the additional overhead involved, if the data is worth gathering. An option should also be able to either include all security profile maintenance in this audit trail or in a separate "Profile Trail."

Authorization Scope — The installation should be able to select the scope of authorization by resource type. For example, if only data set authorization is desired, then code for program, terminal space allotment authorization, etc., should be omitted from the system.

Data Set Sanitization — In addition to individual data sanitization requests made by the user in his job, the SSS should provide a capability for blanket sanitization based on one or more criteria. These criteria may range from security levels assigned to data sets, unique qualifiers in data set names or profile data set grouping. Again, this feature should be a selectable item.

Hardware Bugger Sanitization — This capability should be chosen by device type or specific unit address. Thus, only those devices potentially handling some type of protected data need be sanitized upon deallocation.

Security Profile Considerations —

The profile should be capable of storage on any type medium.

It should have the flexibility to be shared between CPU's.

The installation should be able to select whether the software system will maintain a current standby profile in the event the primary profile becomes disabled.

Data Set Name by Volume — The installation should be able to choose whether it intends to control data sets by name only or by name and volume residence. The latter restricts the number of copies of data in existence. This feature should be optional because it could have a significant impact on the amount of work necessary to establish and maintain the profile.

Sub-system Interfaces — Even though a software security system will in most cases be executing in an environment with one or more sub-systems, these sub-systems may not require an interface to the security system. The installation requiring no interfaces should be able to eliminate that code from the production system at SYSGEN time. (Note, however, that the security system should contain one common interface for all sub-systems. This means that if only one of the sub-systems requires the interface, it must be included.)

Resource Restriction Methods — Three major approaches can be used in relation to resource restriction methods. A software security system can operate with either a total resource *inclusion* technique or total resource *exclusion* technique or a *combination* of both.

The *inclusion* technique allows all system resources to be available to all system users unless a resource is specifically defined as restricted.

The *exclusion* technique restricts all system resources from all system users unless specifically defined as being accessible. (This technique in its pure form has limited use since it requires all resources within the system to be controlled.)

An example of a useful *combination* of both follows: A software system could provide the inclusion technique for general use, but use the exclusion technique for resources which meet certain criteria. This criteria might consist of selected qualifiers for data set names, selected controller addresses for sets of terminals or perhaps selected qualifiers for program names. Many criteria could be established.

The important point in this area is that a software security system should provide the SYSGEN capability to mold the restriction methods available into *one* which is unique to the installation's requirements.

Level of Administrative Control — Perhaps the most important function to contain flexibility is the level of security support provided to the security office. This level of support pertains exclusively to the varying methods by which the security profile may be updated from an administrative viewpoint. Three basic categories of support are possible.

Centralized Profile Method [*CPM*]
The CPM is characterized by the dominant role played by the installation security office (ISO). This office gathers all user requirements and transcribes them into profile update commands. The ISO is essentially the security middleman between the system and the user. This method places increasing demands on the ISO as the users' organizational complexity and security requirements expand.

Subordinate Profile Method [*SPM*].
The SPM differs from the CPM in that subsecurity offices are possible. These suboffices may be established along the organization paths of the installation's users. The ISO then defines bounds within which each suboffice may update and interrogate the security profile. Each suboffice handles its own requirements without impacting the others. The ISO may or may not have access to suboffice recorded data within the profile depending upon installation requirements.

Decentralized Profile Method [*DPM*].
Certain environments require a DPM. This method deviates from the others in that the profile updating is done by the user within his job based on his requirements. The security office in this environment will have less user responsiblity because it now only monitors user profile status and requests rather than performing all updates.

- *Automatic vs. User Functions*

The system should provide flexibility between those security functions which are automatically performed and those which are executed upon *user* request only. For example, an installation may wish to leave data set sanitization decisions to the discretion of the user. The user would then issue the request within his job. Another installation, however, may not wish this decision to be made by an individual user. In this case, the sanitization would be automatically performed upon deletion of every data set meeting the predetermined criteria.

In determining which method to use, the installation must review the number of users and resources to be included in the profile along with organizational characteristics. This data should be fitted with desired points of control within the organization. As one example, in the CPM, the ISO has full control but may not be able to quickly respond to user requests in a large, complex installation.

- *Education Requirements*

The disciplined environment which must be established with the installation of a software security system includes adequate education and training at all levels. The amount of education required will vary with the complexity of the software system and the security functions implemented.

The categories of education to be considered include:

Management — The management personnel must understand how the software will function in general terms, what security functions are to be implemented and what actions they must take to support a successful implementation.

Users — Personnel in the using organizations must understand how the software system affects them, what previous practices will no longer be accepted and be aware of all requirements.

Security Office — The personnel responsible for developing and maintaining profiles and auditing the software system functions must be thoroughly versed in security office procedures and administrative requirements.

Software — The software personnel must be technically proficient in the installation and maintenance procedures of the software security system. In addition, it is essential that the system programmers maintain a continuing dialogue with vendor support personnel concerning the degree of security required and the most effective way to support the hardware/software environment.

Operations — Operating personnel need to be familiar with the new procedures for operating the software security system and the routing of attempted violations printout to the security office.

- COST CONSIDERATIONS

After the software security system requirements are defined, cost considerations must be identified. The costs can be broken into two categories:

Implementation costs
Operational costs

The implementation costs include, but are not limited to the following:

Administration
- Planning
- Budgeting
- Organizing

Procedures Development
- People
- Materials

Education
- Instructors
- Staff cost for attendance
- Materials
- Equipment
- Classrooms

Software Installation
- Planning
- Staff
- Generation
- Testing
- Installation
- Application program change costs (*vis,* the recoding of application programs to run in a secured operating system environment)
- Staff
- Testing
- Planning

As a result of Project SAFE, the efforts to install the prototype software security system was expended in approximately the following proportions:

Software Installation	40%
Administration	25%
Procedures Development	20%
Profile Development	10%
Education	5%

It should be noted, however, that these figures represent "ball park" estimates. It is meaningless to specify the Project's manpower loading figures for the installation of the prototype software security system, because many of the fixes and problems that were encountered and documented would be resolved prior to release of a vendor supported system. The complexity of your operating system and operating environment will also influence, to a large extent, the ease with which you can implement a software security system. In addition, your profile development effort will depend almost entirely on the size and complexity of your security profiles for users of system resources.

The operational costs include:

Administration
- Management attention

Staffing
- Software security system maintenance
- Profile maintenance
- Procedure maintenance
- Security Office operations

Rental/Purchase (amortized)
- Software security system
- Floor space for extra staffing

Education
- Instructor
- Classrooms
- Materials
- Staff attendance

Performance
- Overhead absorbed by computer system
- Degradation billable to users

Inconvenience
- Rerun
- Degradation
- User setup

It is not possible, however, to give cost figures. Cost will vary due to many factors, including installation size and complexity, the number and kinds of security functions used and adaptability of your organization to support a software security system. You must, therefore, plan, budget, and staff your installation for the amount of security you need and can justify considering your vulnerabilities.

Weighing Evaluation Criteria

"How do you compare software security systems on the basis of these evaluation criteria?

The following calculation worksheet for evaluating software security systems is based on a logical sequence of steps and will help you reach a decision. Use of the worksheet is described below.

EVALUATION CRITERIA	CRITERIA WEIGHT (1 - 10) ①	SYSTEM A RATING (1 - 10) ②	SYSTEM A WEIGHTED RATING (1) X (2) ③	SYSTEM B RATING (1 - 10) ④	SYSTEM B WEIGHTED RATING (1) X (4) ⑤
1. Performance					
2. Maintenance					
3. Administrative Support (Procedures)					
4. Impact on Applications					
5. Impact on Operating Systems and Subsystems					
6. Ease of Implementation					
7. Ease of Use					
8. Functional Capabilities					
9. Flexibility					
10. Security Utility Aids					
11. Education Requirements					
12. Cost					
Total Weighted Rating:					

Twelve different criteria are listed down the left-hand side of the worksheet. The first step in using the worksheet is to consider each criterion and rank it on a scale of one to ten in order of importance to your operating environment. A very important criterion would be given a rating of 8, 9, or 10; a criterion of very little importance would be given a rating of 1, 2, or 3, for example. Put the rating figure in column one.

Then, consider System A in terms of the various criteria. In column two, give the system a rating for each of the criterion which you have just evaluated for your environment. What importance does the system place on each criterion — again, rated on a scale of one to ten? If the system is very high on providing maintenance, for example, you might give the system an 8, 9, or 10 rating on maintenance.

In column three, put the product of columns one and two. If the system is doing what you want it to, the number placed in column three should be high. For example, if you rated maintenance as being very important, perhaps an eight, and the system does provide extensive maintenance, again rated eight; then the product in column three would be 64. Another system may provide very little maintenance — rated 3. The product in column three for that system would be 24. For your purposes, System A is the better system. In short, the higher the number in column three, the more the system fits your needs.

There may be additional systems which you want to evaluate against System A — use columns 4 and 5 and any additional columns which you might want to add to produce values for those systems. To compare systems on a gross basis, the totals of the *Weighted Rating* columns for each system should be compared. As a general rule, the system with the highest total is the best system for your environment.

As a word of caution, though, there may be certain criteria which are critical. For example, cost may be the one criterion which would exclude any system which does not fall within the permissible maximum. Or, maintenance may be of the utmost importance. If a vendor does not supply maintenance for the system, there may be a need to exclude the system. For these reasons, simply looking at the totals of one system over another will give you only a gross approximation of the "best" three or four systems. After that, you'll have to make a more thorough analysis of each "best" system. The final selection would include consideration of other factors in addition to those evaluated in the rating scheme, such as:

- Soundness and stability of the vendor
- Industry reputation
- Experience in security software

Recognize that this approach to evaluating software security systems relies heavily on subjective weights and rating. You may justifiably ask, "How can I minimize the effects of my biases and knowledge constraints in order to improve the overall effectiveness of this evaluation procedure?"

One method commonly used to answer just that question is the Delphi Technique, which is discussed in Appendix D. The Delphi Technique can be applied to the first two steps of the software security system evaluation procedure just described, as indicated below:

- The panel, comprised of experts whose judgment is respected by the executive, arrives at a consensus regarding the relative weight of each evaluation criterion for your environment.
- A consensus is then reached on the rating of each criterion for each competing software security system.
- Multiplying the two columns will then provide you with the necessary comparative values.

SSS Implementation Considerations

Careful consideration must be given to the implementation of an SSS, to:

- Minimize the impact on existing levels of computer operating effectiveness.
- Reduce the possibility of "overlooking" specific vulnerabilities and miscalculating the risks involved, and
- Provide for the effective utilization of SSS facilities.

The successful operation of today's computerized information system is a complex process requiring a high level of project control and systems assurance. As with any significant change in the organization's computer operating environment, the implementation of an SSS must be executed in a controlled manner and coordinated with all of the other important activities that typically take place in a progressive information processing establishment. *This is particuarly important because of the broad-based impact of an SSS on personnel and the total system.*

Software security, by virtue of its presence within the computer operating system, must be considered for its potential impact on some of the non-security related aspects of the system. Security at the expense of impaired operational efficiency, productivity, and accuracy is a tradeoff to be balanced and necessitates top management involvement to protect the overall effectiveness of the computer utility. At the same time, management must ask for and receive some assurance that what has been planned for in the way of software security provisions do in fact become reality. The system that creates a false sense of security is potentially harmful. Action should be taken to assure that implementation of SSS facilities do in fact provide the required level of information protection and that it has been achieved in the most efficient way possible.

The successful implementation of an SSS is characterized by:

Careful Planning
Comprehensive Education
Well-Documented and Enforceable Procedures

To ease the implementation and minimize the impact on existing levels of computer operating effectiveness, proper *planning* is necessary. Some specific areas for concern are:

- What **priority** does the SSS implementation have in relation to other organization objectives?
- How will the SSS implementation impact user **information system development plans** and vice versa?
- How will the SSS implementation be **controlled** and who will be responsible for **communicating project status** to management and the user community?
- What are the **roles** to be played by each member of the **organization** during the SSS implementation?
- How is a **security conscious attitude** maintained both during and after implementation of an SSS?
- How will provisions for **tighter system integrity** impact users of the SSS? What plan of action is necessary to minimize this impact?

- Does this plan include:

  Reviewing what facilities are being used and identifying the users?

  Identifying programs that use "back door" facilities of the operating system (vis, use of unsupported or installation supported "hooks")?

  Identifying programs that are "bending" the rules (i.e., fetch protect)?

  Reviewing potential incompatabilities with sub-systems (teleprocessing, installation utilities, other vendor's software)?

  Use of coding standards?

  Identifying information resources to be protected?

  Establishing responsibility and ownership of information?

  Resolving information sharing conflicts?

  Assigning information access capabilities and their type to users?

  Developing security profile of the installation's resources and their use?

  Establishing procedures for the maintenance of the security profile?

- How and to what extend should **extended security facilities** (e.g., controlled access provisions and data set protection) of the SSS be used? What plan of action is necessary for their effective use?
- What will be the impact of the SSS on **user billings**?
- What will be the impact on user **test procedures**?
- What **contingencies** should be established for a backup operating system if major problems arise in the implementation of the SSS?
- How should **incompatabilities** between the two systems be handled? (i.e. changes made to JCL that are not supported by the backup operating system such as codewords on the Jobcard)

Sufficient **education** on the SSS for all affected personnel is necessary to generate a security conscious attitude. Getting your people to willingly work *with* the implementation, rather than against it, will contribute heavily to their ultimate acceptance of the SSS. A good education program — established prior to the implementation — is required to provide the necessary skills for the support and effective use of the SSS facilities. Such an education program will also generate feedback and provide a forum for discussing their suggestions and ideas.

The development of well-documented and enforceable **procedures** to support the SSS is essential and should be addressed during the implementation. Software security is but one link in the chain of protection for the organization and must be coordinated with the establishment of proper administrative procedures and controls to be effective. It has been said that *unless operations management maintains physical, procedural and personnel safeguards, the system's security will constantly be at risk, no matter how much protection has been programmed in.**

HARDWARE SECURITY

The security of computerized information is characterized by a combination of both hardware and software technology. This section is intended to describe briefly the role that hardware plays in the development of an effective computer security program. Specifically,

- What hardware safeguards are available to support the fundamental characteristics of software protection?
- What factors affect the selection of hardware versus software security features?
- How is the effectiveness of software security related to the effectiveness of hardware security?

The development of hardware devices and features to complement the software in maintaining system security is not a new idea. Since the advent of multiprogramming, hardware isolation techniques have become commonplace as an effective tool for protection. Memory partitioning is a good example of this. Privileged machine states and instruction sets are fundamental to the correct operation of today's computing machinery and are for the most part inseparable from the architecture. Other features exist and some need to be developed possibly as alternatives to software security techniques for enhancing the controlled access, identification, and surveillance characterisitics of the system. Following is a list of various hardware devices and features, that contribute to the fundamental characteristics of software protection:

Integrity Features
- parity checking circuitry
- store protection (write inhibit)

Isolation Features
- privileged machine states
- privileged instruction sets
- memory partitioning/bounding
- main memory block erase
- dedicated memory (multiprocessors)
- print inhibit capability on hardcopy terminals

Controlled Access
- tape volume protection rings
- DASD write inhibit switch
- cryptographic encoding devices
- terminal locks
- fetch protection (read inhibit)

Identification
- terminal badge reader
- card input device badge reader
- positive hardware identification of terminals and peripherals

Surveillance
- Security Office terminal
- alarm devices
- DASD check sum logic
- Test Protection instruction
- minicomputer threat monitor

Determining whether hardware or software features should be selected to execute a prescribed security function depends on the availability of the feature, its cost, efficiency and effectiveness as a threat deterrent.

It should be noted that the effectiveness of total system security will require understanding the working relationship between the system hardware and software. The dependency of system software on machine hardware for the reliable execution of the programmed security controls is fundamental and must be considered for its potential impact on the integrity of a software security system. This concern has been previously expressed by L. M. Mohlo in *Hardware Aspects of Secure Computing:*

> *Software access controls rely upon certain pieces of hardware. If these go dead or be deliberately disabled without warning, then all that remains is false security.*

Exposure as a result of hardware failure is possible through design flaws and improper maintenance. Hardware subversion techniques include the temporary disablement of protection features or countermeasures and will require additional administrative policies and procedures to check the potential threats.

**SECURITY & PRIVACY IN COMPUTER SYSTEMS* Anthology, Lance J. Hoffman — Security Considerations for Operations Management, IBM G520-2169-0

PHYSICAL SECURITY

A balanced security system must include appropriate physical safeguards in addition to software protection. In considering physical security, just as in software security, the manager is confronted with rapid technological advances in equipment and security systems and increasing numbers of hazards. This combination can subject the security system to obsolescence in a relatively short period of time.

This review of physical security is divided into four segments:

Physical resources to be protected

Hazards to be protected against

Protective measures to be considered

Information storage and disposal management

- Physical Resources

Two kinds of questions are related to the consideration of physical resources:

What specific resources are to be protected?

How important is protection of those resources to the organization?

The specific resources to be protected include:

Computer and peripheral equipment

Support facilities

Data media

Libraries

Documentation

Personnel

In analyzing the need for physical security protection, a number of factors need to be considered. The ability of the organization to finance prompt recovery from loss is one factor. Are contingency funds available or is insurance coverage adequate? The criticality of the information service being provided must also be considered. Is your situation such that alternate processing would have to be performed almost without regard to cost? Is contingency planning adequate and what are the expected costs of purchasing temporary services and re-establishing the facility?

A more thorough examination of the approach to analyzing the trade-offs between consequences of loss versus security cost, is presented in the chapter on *The Economics of Security*.

- Hazards

The development of physical safeguards must consider the likely hazards to which the installation may be exposed. The following list includes some possible hazards:

Accidental destruction such as fire, water, wind, earthquake

Mechanical interruptions such as equipment failure or utility loss (e.g., power, water, communications)

System losses resulting from various actions including accidental modification of equipment and support facilities

Accidents during maintenance, repairs and enhancements

Operator errors disrupting equipment, data, programs and software

Accidental disclosure resulting from lost keys, lock combinations or identification badges

Intentional disruption by dissident employees or outside personnel

- Protective Measures

In addition to the cost factors of physical security, another consideration is the compatibility of the security program with the installation's primary functions. Extreme measures to attempt complete protection may introduce restrictions and rigidity that would be self-defeating by limiting the capability of the facility. A number of reasonable protection measures may be considered.

When a new facility is being planned for the data processing function, important factors to consider include:

Site selection is a key consideration and the manager enjoys greater flexibility today than ever before in selecting a site for the data processing installation. With past technology, it was important for the installation to be physically located as near as possible to the users. With telecommunications capability this requirement is considerably diminished and security considerations actually favor a remote processing site. The trend today is toward isolation of the data storage and the central processors while geographically distributing the peripheral devices closer to the users via data communication lines.

Architectual design is another important factor. Physical provisions for restricted access can be incorporated into the design. The concept of a "blockhouse" — a one-story, windowless and limited entry/exit structure — is becoming increasingly popular. Protection and "fail safe" design of the support facilities are additional design requirements.

When a new facility specifically designed for the data processing function is not feasible, major considerations include:

Avoid below ground level facilities or other sites which are subject to flooding. Automatic pumps and drains are subject to failure under extreme conditions. Flooding has been found to be the greatest cause of insurance claims. This situation is primarily due to poor site selection and association with other machines which are normally put in the basement.

Windows should be avoided because of vulnerability (ease of ingress and breakage), loss of usable floor space, and the necessity to combat solar heat.

Avoid sites in buildings open to the general public to minimize the exposure resulting from public traffic. Public reference to the location of the data processing facility should be avoided to minimize the challenge that security access control systems represent to some individuals.

Sites should be located approximately in the center of the building to utilize the maximum inherent protection of the structure, but generally not higher than eight to ten stories. Passenger and freight elevator service must be adequate.

The site location should consider availability of fire and police protection, outside utilities, and equipment service centers.

Administrative procedures are widely used to solve security weaknesses, but are generally less effective and reliable than physical measures. Personnel turnover, changes of management and their policies and priorities, office rearrangements, changes of functions in adjoining areas and changes of building management practices undermine the enforcement procedure. If procedures, controls, inspections and preventive measures are the basis of security, the effort will depend largely on the committment of top management. This committment implies allocation of sufficient staff to develop and maintain a coordinated and well-balanced program.

Uninterruptable power systems are being employed in a few large installations with general success. Reluctance to acquire more of these systems stems from high costs, space and the initial installation problems. Cost is approximately $1,000 per KVA, plus the loss of space and the nuisance of the generators. Some installations have experienced down time in the initial phases to offset several years of outages under normal utility power. Most of these problems have been attributed to improper installation and checkout procedures.

Controlled access systems offer a relatively new tool for controlling traffic into sensitive area. These systems normally include small computers used in combination with magnetically coded badges, closed circuit television, turnstiles, audit trails, vibration and detection devices, etc.

The isolation of the processors and data media for security purposes generates a greater dependence upon communication, transmission, and remote terminal facilities. These are areas over which data processing usually has little control. Switched network capability and alternate lines and terminals offer some alternatives, but generally are expensive and are of little value against intentional disruption. The terminal facility encounters the same hazards as the central facility and must, therefore, be considered in the same manner.

- Information Storage and Disposal Management

Information storage and disposal management are key elements in planning physical security requirements. Why is there a need for information storage and disposal management controls? Consider, for example, the financial department in your organization. It probably keeps all vital records locked up and away from unauthorized personnel. The same should hold true for data processing files considering their criticality to the functioning of your organization. Improperly discarded confidential data presents opportunities for competition to gain trade secrets or for violation of an individual's right to privacy.

What controls are required for information storage and disposal management? The answer to this question requires a complete analysis of your organization to make certain that all uses and users of confidential data are identified and authorized.

The following categories of data should be protected:

Current files

Backup files

Procedures and programs

Confidential obsolete and extraneous information trash

What controls are required to protect this data? The determination of the controls required will necessitate reviewing your organization's work flow and backup storage facilities. The controls that are to be established must not hinder the work flow, but should aid in the work being performed in a more orderly or controlled manner and directly relate to the controls and protection systems included in physical plant control. Some additions to physical plant controls to consider are:

On-site or off-site fireproof storage

Storage in on-site isolated locations

Storage in off-site remote locations

Procedures concerning the utilization of stored data

Another area often overlooked is control of confidential obsolete and/or extraneous information trash. Most computer-generated reports are eventually discarded. Computer operators will make mistakes in aligning new forms in the printers or starting new jobs and will discard the forms after restarting the job. This discarded material represents a potential security leak.

When analyzing trash control security requirements, several tools should be considered:

Compactors to prevent casual browsers from acquiring information from waste containers

Shredders to make reconstruction of reports virtually impossible

Incinerators to destroy all traces of information

Procedures to instruct how and when to use the disposal devices

In addition to these tools, periodic audits should be conducted to assure that confidential data is being disposed of properly.

LEGISLATIVE CONSIDERATIONS:

RECORDS, PRIVACY AND THE LAW

The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.

One might expect these to be the words of a radical civil libertarian. However, this quotation is taken from an article entitled *The Right To Privacy* which was published in the *Harvard Law Review* in 1890 and co-authored by the eminent legal scholar, Louis D. Brandeis.

It is apparently a popular misconception that the right of an individual to be free from unreasonable intrusions into what is commonly understood to be the private or personal sector of his environment is a recently developed concept — a concept which is much discussed, but which has not yet attained the status of a right, recognized and protected by the law. As evidenced by the Brandeis quote, however, farsighted legal commentators have, for some time, recognized, what Justice William O. Douglas later referred to as the "penumbras" of the right to privacy in the existing body of constitutional and common law. The right to privacy is present, real and enforceable. However, in order to properly understand the nature, limitations and future of the right to privacy, you should be familiar with its development and its current status in the area of constitutional, common and statutory law.

CONSTITUTIONAL LAW

In America, the concept of a right to privacy springs from the American colonial resentment toward general warrants for search and seizure issued by the British Governors prior to the Revolutionary War. This attitudinal reaction against invasion of home and seizure of personal property was formalized in the 4th Amendment to the United States Constitution, which guarantees *the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search and seizures . . .*

Until relatively recent Supreme Court rulings, the constitutional rights granted by the 4th Amendment remained mere property rights assuring a citizen freedom from physical interference and trespass. However, as noted by Warren and Brandeis, in their 1890 commentary, *political, social, and economic changes require the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.* It was not until very recently, however, that the United States Supreme Court, in decisions involving alleged violations of the 4th Amendment rights, abandoned the traditional restrictive interpretation based on property rights.

In its 1967 decision in *Katz* v. *U.S.*, the Court recognized society's need for an expanded interpretation of the 4th Amendment Rights. It held that the electronic surveillance of a public telephone booth without a warrant constituted an unconstitutional search and seizure. The United States Supreme Court extended the constitutional protection beyond a mere property right to include what one seeks to preserve as private, even in an area accessible to the public. The Court thus acknowledged that the constitutional right to be free from unreasonable search and seizure belongs to the person and not to his property. Further, the Court acknowledged that he should be entitled to that right wherever and whenever he has a reasonable expectation of privacy. This expansion of the 4th Amendment rights to include intangible things (e.g. conversations) could not have been foreseen by the draftors of the Constitution since it was a reaction to technological advancement unknown to them.

Perhaps the most significant Supreme Court decision on the constitutional right to privacy is that Court's ruling in *Griswold v. Connecticut.* The primary significance of the Court's holding in *Griswold* is that for the first time, the Court recognizes a right to privacy outside of circumstances involving searches or seizures in violation of the 4th Amendment. Specifically, the Court ruled unconstitutional Connecticut's anti-birth control legislation which prohibited physicians from advising, examining and prescribing birth control devices for married persons. The Court reasoned that certain activities, not specifically or expressly guaranteed under the Bill of Rights, have been recognized as constitutionally protected forms of expression. The Court found that rights of privacy were impliedly protected by the 1st Amendment (right of association), the 3rd Amendment (prohibition against quartering of soldiers in private homes), the 4th Amendment (prohibition against unreasonable search and seizure), the 5th Amendment (prohibition against involuntary self incrimination) and the 9th Amendment's reservation to the people of unenumerated rights.

The *Griswold* decision signaled the beginning of a prolific era of litigation characterized by a heightened consciousness of the right to privacy. This phenomenon is evidenced by a deluge of decisions from jurisdictions across the country dealing with criminal prosecutions or governmental investigations of sexual habits and relationships, legislative prescriptions regarding personal safety and regulations with respect to the length of a student's hair. Insofar as these cases represented opportunities for the Supreme Court to further refine its posture with respect to the right to privacy, the court declined to consider most of them.

Ultimately, the ferment which the Court set in motion with its decision in *Griswold* culminated in its recent, highly controversial decision regarding a woman's right to determine whether or not to terminate her pregnancy by abortion. Recognizing a mother's right to privacy, the Court found a Texas statute prohibiting abortion to be unconstitutional.

Based on the Court's apparent alacrity in safeguarding the individual from various forms of intrusions upon his person, property and intangible elements of his environment, one might anticipate a logically resultant willingness to protect the individual from governmental or private intrusion by way of record and information collection. In fact, early decisions of the Court were indicative of such a trend. However, initial rulings limiting governmental inquiries and information collection have been overshadowed by later decisions.

Recent cases reinforcing the government's right to know, hold generally that the government may require the production of relevant information wherever it may be and regardless of the form in which it is maintained.

Courts are particularly willing to require production where the government's revenue interests are at stake. The Census Bureau may collect data without warrant; however, Congress has established a statutory prohibition against the raiding of Census Bureau information by other federal agencies.

Some narrow limitations have been placed on the governmental right to know. Thus, the Secretary of the Treasurer may not, under the auspices of the Bank Secrecy Act, require routine reporting of domestic financial transactions without summons, subpeona or warrant where the material requested is irrelevant to any matter under inquiry.

Although some decisions recognize a limited corporate constitutional right of privacy, it is generally held that since corporations are clotted with public attributes and have a collective impact on society, from which they derive the privilege to act as an artificial entity, the corporation's right to privacy is much more limited than the individual's.

An area of considerable controversy and commentary is the question of an individual's constitutional right to privacy with respect to credit and insurance investigating bureaus. The primary impediment to recognizing a constitutional right to privacy in this area is the absence of state action. It is, of course, a well established principal of constitutional law that the Bill of Rights protections are generally available to the individual only as against state or governmental action. Although some legal commentators have theorized that the activities of information collectors are so related to governmental policies and so impregnated with governmental character as to satisfy the requisite state action. However, the present state of law offers very little real constitutional protection, even as against the government, with respect to information gathering and collection. In the vast majority of instances, Courts, balancing the individual's right to privacy against the government's right to know, have favored the latter.

COMMON LAW

In addition to the principles of constitutional law guaranteeing a right to privacy, there has developed a body of common law which affords the individual a remedial action against one who violates his right to privacy. This body of law defines actionable intrusions on one's privacy and distinguishes them from those not recognized as actionable.

The concept of a remedy for actionable or tortious invasion of privacy (it is generally agreed) stems from the Warren-Brandeis *Harvard Law Review* article discussed above. Since 1890, the vast majority of jurisdictions have recognized a common law right to privacy in one form or another. By 1960, a renowned legal scholar in the area of tort law counted 35 jurisdictions which recognized actionable violations of the right to privacy, and classified four distinct causes of action which had developed. Although some commentators have challenged this classification, it is worth noting here, because it is indicative of the scope of recognized actionable offenses:

- Appropriation for one's benefit or advantage of another's name or likeness.
- Intrusion upon one's physical solitude or seclusion.
- Publication of a highly objectionable kind relating to private information about another.
- Publicity which places one in a false light in the public eye.

Apparently only three states continue to reject the existence of a common right to privacy: Rhode Island, Wisconsin and Nebraska.

As with respect to the constitutional right discussed above, the common law right to privacy is not absolute and the individual's right to be left alone must be balanced against and harmonized with community interests and the right of other individuals to know and publish. Since examples of Court decisions relating to various circumstances should help to illuminate the vast scope of circumstances to which the common law right to privacy is presently being applied, the following sampling of rulings is included for that purpose and to outline the historical development of the common law regarding privacy. It must be emphasized however, that these are merely cited as examples and, because of the vast disparity in rulings among various jurisdictions and the general lack of definitive pronouncements from United States Supreme Court, these holdings can by no means be relied upon as currently representing the state of the law in all jurisdictions.

- In 1962 a Federal Court applying state law, found that a cause of action has been established where a tire dealer who, under the mistaken belief that the claimant was not current on his tire payments, removed all four tires from his car and left it in a parking lot on its wheel rims in full view of the claimant's fellow employees and others. Under similar circumstances, decisions frequently turn on whether or not the exposure is found to be objectionable to a reasonable man of ordinary sensibilities. Applying the same standards, however, Courts have found that an employer's publication of an employee's wages is not offensive to a reasonable man.

- A California Court, adopting what has been labeled a minority position, recently allowed recovery for an alleged unnecessary use of the claimant's name in a publication reviving past events. In that case, the defendant had published an article on truck highjacking which using the claimant's actual name, related an incident, for which the claimant had been convicted 11 years earlier. The plaintiff claimed that as a result of the publication he was scorned and abandoned by his family and friends. The Court, balancing the individual's right of privacy against the general interest in an unfettered press, held that under the circumstances before it, the former outweighed the latter.

- A large number of cases have considered invasions of privacy based on physical intrusions, usually overzealous and physical peeping, spying or eavesdropping. Probably the most controversial example of actionable intrusion by surveliance is the decision of a New York Federal Court in *Gallela* v. *Onassis*. In that case, suit was brought by the plaintiff-photographer who claimed that Jacqueline Onassis and her Secret Service Agents were liable for interferences with his business, false arrest and malicious prosecution. Mrs. Onassis, the defendant, filed a counterclaim against the plaintiff based upon an alleged violation of her privacy, under both common law and constitutional law. In addition to finding that Mrs. Onassis was entitled to a cause of action for assault and battery, the Court found that the plaintiff-photographer had committed actionable intrusions upon Mrs. Onassis's privacy. The plaintiff-photographer had allegedly pursued Mrs. Onassis and her children photographing them at close distance in theaters, restaurants, parks, schools and tennis courts, using derisive language as he leaped about them. Despite the fact that the defendant was found to be a public figure, the Court held that the plaintiff-photographer has "no general constitutional right to assault, harass or unceasingly shadow Mrs. Onassis". The *Gallela* case is of particular significance for the reasons that it extends the right of privacy to public figures in public places and more importantly dovetails the common law and constitutional grounds for relief.

An increasingly large number of cases dealing with the common law right to privacy involve allegations of intrusions by way of commercial or governmental information collection and credit reporting. Claimants are, however, almost universally unsuccessful in obtaining relief under the current state of the common law right to privacy. A general rule has developed that no cause of action would allow for intrusions for the purpose of collecting information unless such intrusion is extreme and unreasonable.

- One example of such a case is the ruling of a Federal Court in South Carolina that the agent of a credit reporting company acted in good faith and in pursuit of what the Court called the legitimate goal of collecting information in a routine insurance investigation. In that case, the plaintiff alleged that he had been exposed to physical and mental suffering and extreme embarrassment by reason of the agent's coming to the plaintiff's home and questioning the plaintiff's wife regarding matters such as her age, the number of children in their family, the plaintiff's salary and the plaintiff's present insurance coverage. Similarly, where an action was brought alleging that the defendant — a Retail Store — had informed a credit bureau of a disputed delinquency in the plaintiff's account, the Court found no actionable violation of the plaintiff's common law right to privacy. This was true even though the account had, in fact, been opened by one fraudulently using the plaintiff's name and due to the false credit report the plaintiff had been required to the first time in his life to furnish collateral for a loan.

Typically, Courts rule against plaintiffs in credit reporting privacy cases on the basis of a qualified or a conditional privilege which stems from what is recognized to be society's legitimate interest in collecting information. Generally, in order to be actionable such an intrusion must be physical and akin to trespass. The mere submission of a confidential credit report to those with legitimate business interests — even if false — is generally not actionable under the current state of the law. Courts typically hold that where there is no publication, public surveillance, constant harassment or trespass; society's commercial interest in obtaining credit information should be recognized as paramount. The outcome is usually the same where the action is based upon libel or slander unless there has been a publication of defamatory matter not reasonably necessary to accomplish the business purpose or unless derogatory or defamatory information has been sent to disinterested subscribers or members of the public.

In summary, actions against credit reporting bureaus for intrusion upon one's privacy require acts of physical harassment which are objectionable to a reasonable man of ordinary sensibilities. Recovery may be allowed for over-zealous physical surveillance and unauthorized wire tapping or electronic surveillance; but the mere questioning of one's family or friends is generally not actionable. The questions which an individual must answer in order to obtain credit, apply for a job, or enroll in a school are normally entitled to a qualified privilege. Suits alleging publications of private facts by credit reporting bureaus are frequently not successful because the information is transmitted to "interested subscribers" and not released to the general public. Additionally, facts obtained from others are held not to be private facts simply because someone else already knew them. One commentator has summarized the current state of the law as follows:

The established tort doctrine relating to our problem may be summarized as follows: If accurate information is disclosed out of the subject file, there is no liability unless disclosure is made to a great number of people, however sensitive the information may be. Since disclosure of such information is normally made to professional investigators, the remedy of damages for invasion of privacy offers little protection to the subject, and even though the information be arguable false, the disclosure will be qualifiable privileged against an action for damages on a defamation theory so long as the investigation is, or represents, a prospective lender, a wife seeking evidence in a divorce proceeding, a prospective insurer or some one else who has what the law regards as a sufficient interest in inquiring — assuming that the information disclosed is relevant to that interest. The kind of rigid limitation and access to sensitive personal information that would be needed in order to give the subject effective protection against improper disclosure of personal data is thus uncongenial to existing theories of recovery of damages for defamation or invasion of privacy.

Thirty-one Law and CON. TROB. 342, 347.

An overview of the right to privacy as it is defined in the bodies of constitutional and common law reveals an almost universal recognition of the right and a trend toward an expansion of the scope of circumstances under which the right may be enforced. There appears, however, to be an exception in cases involving intrusion by credit reporting companies. It is, in fact, difficult to find a pattern or a trend in the development of the law of privacy relating to credit reporting. If there are to be any significant changes in the current state of the law in that area, they will undoubtedly come in the establishment of stricter standards imposed upon credit-reporting companies rather than in the abandonment of the qualified privilege now enjoyed by such companies. Although the imposition of a requirement of a higher standard of care would, in the technical sense, afford the individual increased protection, such a measure would, as a practical matter, be of dubious value. This is true because the injured person would be required to bare the burden of establishing details and specific facts showing a failure on the part of the reporting company to meet the higher standard of care. This involves considerable time and expense and there is, of course, little certainty regarding the manner in which the trier of fact will view the circumstances.

In any event, it must be recognized that the common law and the constitutional right to privacy is not a mere fantasy or dream. It is real and present and the manner in which it is applied by the Courts in response to increasing societal pressures is significant to all of us.

STATUTORY PROVISIONS

In some instances responding to developments in the constitutional or common law right to privacy but far more frequently responding to their constituents, the United States Congress and the legislatures of the various states have enacted legislation relating to privacy. The following summary reviews some of this legislation — while not exhaustive, it is exemplitive of the broad scope of such legislation.

FEDERAL STATUTORY PROVISIONS

Two Federal statutes contain specific recognition of the right to privacy. They are: The Fair Credit Reporting Act, and the Freedom of Information Act. These and certain other statutes and statutory provisions are described in this section.

• **The Fair Credit Reporting Act** deals with the collection, maintenance and distribution of consumers' credit reports which are used, at least in part, for determining the consumer's eligibility of employment, credit or insurance. The Act does not apply to reports used for business, commercial or professional purposes. In its statement of purpose, the Act specifically recognizes a right to privacy with respect to consumer credit reports:

There is a need to insure that consumer reporting agencies exercise their grave responsibility with fairness, impartialty, and respect for the consumers right to privacy.

The Act imposes a limitation on the period of time that a credit reporting agency can hold any bit of information. When this time limit expires, the data becomes stale and cannot be disseminated unless the report is to be used for determining whether to grant credit in excess of $50,000, underwrite a life insurance policy having a face value in excess of $50,000, or offer employment carrying a compensation in excess of $20,000 per year. Where credit or insurance for personal, family or household purposes or employment is denied or the charge for such credit or insurance is increased, wholly or partly because of information received from a consumer reporting agency, the user of the consumer report must advise the consumer and supply the name and address of the reporting agency. This is also true when credit is denied, wholly or partly because of information bearing on the credit-worthiness of the applicant. If the information has been obtained from a source other than a consumer reporting agency, the user of the information must disclose its nature upon written request of the consumer. In most cases, a person procuring or causing to be prepared an investigative report about a consumer must so notify the consumer. The Act provides that a consumer reporting agency is to follow reasonable procedures to insure the maximum possible accuracy of the information contained in such a report. Upon the request and proper identification of any consumer, the reporting agency must clearly and accurately disclose the nature and substance of all information (except medical information) which it holds and the sources (except sources gathered and used solely for the purpose of preparing an investigative report) of such information. Of course, this provision does not give the consumer the right to physically possess the file or receive a copy of it, only the right to know its contents.

In the case of a dispute between the consumer and the reporting agency, the agency is required to reinvestigate the accuracy of this information. If the dispute remains unsolved, the reporting agency must so note the dispute in subsequent reports. If disputed information is deleted from a file the reporting agency must so notify certain persons designated by the consumer who have received the reports. With a few exceptions, the consumer reporting agency may impose a "reasonable" fee for making disclosures pursuant to the Act. The Act provides civil and criminal penalties for violations of its provisions. Compliance is enforced by the Federal Trade Commission.

This brief statement, highlighting certain provisions of the Fair Credit Reporting Act is intended as a mere illustration of the scope of the Act and it must be borne in mind that complete compliance with the provisions of the Act requires a more detailed analysis and expert advice.

• **The Freedom of Information Act** which generally provides for public access to records held by governmental agencies, also recognizes the individual's right to privacy:

> *. . . to the extent required to prevent a clearly unwarranted record invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, stigma of policy, interpretation, or staff manual or instruction. However, in each case the justification for the deletion shall be explained full in writing . . .*
>
> 5 U.S.C. ¶ 522 (a) (2)

Although the statute, which provides a procedure whereby an individual can prevent sexually-oriented advertisements from being mailed to him does not expressly mention the right to privacy, that right was expressly stated by Congress to be the reason for the enactment of the statute. Thus, Congress found:

> *that such use of the mails constitutes a serious treat to the dignity and sanctity of the American home and subjects many persons to an unconscionable and unwarranted intrusion upon their fundamental right to privacy.*

The first type of statute referred to above is what is sometimes referred to as the **Public Records Act** (44 U.S.C. ¶ 3501, ET SEQ.) That Act provides for certain limitations on Federal agency information collection practices. The pertinent section of the Act reads as follows:

> *A Federal agency may not conduct or sponsor collection of information upon identical items from ten or more persons, other than Federal employees, unless, in advance of adoption or revision of any plans or forms to be used in the collection . . . The Director has stated he does not disapprove the proposed collection of information.*

Examples of similar legislative controls include: limitations on the use of census data obtained under the Census Act; the required confidentiality of information obtained in the course of venereal disease prevention control projects and programs; grants for research treatment and control of sickle cell anemia and Cooley's Anemia; educational and research programs of the Attorney General concerning drugs and other controlled substances; and grants from the Secretary of Health, Education and Welfare for programs in juvenile delinquency control.

STATE STATUTORY PROVISIONS

The Constitutions of at least six states contain provisions which protect their citizens from unreasonable invasions of privacy (Alaska, California, Hawaii, Iowa, Illinois, and South Carolina.) Perhaps the most broadly stated provision is that found in the California Constitution, which states:

> *All people are of nature free and independent and have certain inalienable rights, among which are theirs of enjoying and defending life and liberty . . . and pursuing and obtaining . . . privacy.*

A lack of definitive judicial pronouncements relating to these constitutional provisions prohibits an accurate generalization with respect to their significance.

The various types of State statutory enactments afford protection against certain specific violations of the right to privacy. Several state legislatures have, for example, enacted laws prohibiting the unauthorized use of another's name or image for commercial purposes. Other statutes specifically prohibit unreasonable interceptions of communications.

The only state which expressly recognizes a right to privacy with respect to credit reporting is the State of New York. New York's Credit Data Reporting Act prescribes limitations on what can be included in a credit report and limits those to whom credit rating agencies may give information. This Act, which may prove to be a precedent for legislation in other states, provides for both civil liability and criminal penalties for violations of its provisions.

Responding to a recent survey by the National Association for State Information Systems (NASIS), ten states indicated that they had legislative or administrative policies governing the handling of personal data and state information systems. These policies have as their principal purpose the governing of information practices in the public sector. An example of such a policy is that contained in the **California Budget Act of 1972** which prohibits any expenditure of funds on data processing activities without a certification from the director of the agency involved and the Director of Finance that adequate safeguards have been established to insure the confidentiality of data. The confidentiality criteria used in the State of California are as follows:

- All designers of information systems shall include in their analyses the recognition of the use of confidential information.
- Strict controls shall be developed to prevent unauthorized access to data maintained in computer files. These controls shall include physical security of program documentation, data files, and data processing facilities as well as electronic controls to prevent accidental or intentional unauthorized access to data.
- Each state department shall designate an Information Security Officer who shall be responsible for implementing state policies and standards regarding the confidentiality and security of information in his respective department.
- Each consolidated data center shall also designate an Information Security Officer to carry out the above duties for each data center.

- It is the intention of this Legislature that the Department of Finance continually review the adequacy of state policies and procedures with regard to the confidentiality of data. A report shall be submitted to the Joint Legislative Budget Committee and the fiscal committee on December 1, 1972 regarding progress in this area.

- In order to preserve the integrity of the security and confidentiality measures integrated into the state's automated information systems, any contractor engaging in systems analysis, programming, or other EDP work for the state must hold confidential the details of the work performed, and appropriate language shall be made a part of any such contracts.

Despite the existence of constitutional safeguards in six states, most of the privacy protection afforded on the state level comes from an amalgam of provisions which protect specific relationships or govern the use of personal information held by some department of state government.

There is a great deal of variation among the states with respect to the amount and quality of protection provided for any given privileged relationship and in the amount and quality of protection provided with respect to the various types of personal and business information held by state agencies.

Various relationships have been deemed so important to society that the individuals involved are given protection against in-court disclosure of communications which are part of that relationship. To the extent that the parties to privileged communications may rely upon a freedom from coerced disclosure of those communications, these provisions afford some measure of privacy. It should be noted, however, that a complex body of law has developed as a result of the recognition of privileged communications and the exceptions and limitations are considerable.

The most common privileged relationship is that which applies to communications between husband and wife. The state of Iowa recognizes privileged communications between parent and child and in California communications between guardian and ward are also confidential. The doctor-patient privilege is recognized in some thirty-six states and an increasing number of states recognize a psychiatrist-client or psychologist-client privilege. Other commonly recognized privileged relationships are that of attorney-client and Priest-penitent. Among the privileged relationships which are recognized in some jurisdictions, but remain uncommon are: Dentist-patient, social worker-client; marriage counselor-client; student counselor-student; accountant-client; media employee-source. Numerous state statutes afford a degree of confidentiality with respect to information or data in the possession of governmental agencies. At least nineteen states have enacted general prohibitions against access to identifiable information about recipients and applicants for public aid. Eighteen states provide confidentiality relating to various phases relating to the mentally ill, information obtained through state administration of vocational rehabilitation, certain information obtained regarding persons on parole or probation, certain criminal records and, the records of certain court proceedings involving minors. Still other state statutes limit access to data regarding communicable diseases, complaints of discrimination, disciplinary proceedings in the legal profession, motor vehicle accident reports, information concerning the uses of narcotic drugs or controlled substances, data relating to unemployment compensation, information regarding state or county retirement systems and data acquired in litigation concerning pollution control.

A number of states restrict the use by certain types of businesses of information held in the regular course of doing business. An example of such legislation is a California statute prohibiting collection agencies from publishing or posting lists of debtors commonly known as "dead beat lists" and from engaging in unfair and misleading practices or methods of collection.

To date, no statutes have been enacted which deal comprehensively with the problems relating to the right to privacy in both the public and private sectors. With respect to the public sector, however, a number of noteworthy proposals have been advanced which are designed, at least in part, to guarantee the right to privacy of individuals about whom data is held in state information systems. Some of the proposals have particular relevance to the use of computerized information held in state government data banks. Such proposed legislation frequently contain provisions requiring notification of the existence of a file or disclosure of its existence to a state agency other than by which it was compiled, an opportunity for subject inspection, supplementation, modification and data and periodic purging of data and records.

The foregoing discussion indicates that statutory protection of privacy on the state level is scattered throughout numerous statutes which vary greatly from state to state. Most of the meaningful statutes have been enacted or proposed within the last five years. This is particularly true with respect to the constitutional recognition of the right to privacy. Therefore, it is probably fair to assume that there is a trend toward the enactment of such statutes. Characteristic of the more recent enactments are:

- A clearer recognition of the right to privacy,

- An expanded scope of application and

- More effective sanctions for violations.

With the possible exception of constitutional provisions, the more recent measures tend to deal with both the public and private sectors. In terms of the subject matter of such legislation, a trend appears to be developing toward regulations which protect confidentiality with respect to credit and credit reporting practices and governmental information systems. A final area in which legislation is likely to proliferate is with respect to the confidentiality and practices relating to the maintenance of criminal records, in particular in cases involving minors.

CONCLUSION

The right of privacy, like every other principal of law, is not susceptible to absolutes. It cannot be reduced to a brief unqualified definition and, rather than remaining constant, it is continually changing and developing. This is, in fact, particularly true of the law of privacy which is now in its infancy.

The right to privacy is, in fact, virtually meaningless in the abstract. It takes on real significance only when it applies to a given set of circumstances; whereupon it becomes, for that limited purpose, simply what the court or legislature says that it is.

This section, or any single work or treatise, can adequately impart sufficient knowledge to allow you to know with certainty, precisely, and completely what the right to privacy is and how it applies to the infinite variety of factual settings, which are part of our everyday environment.

It is hoped, however, that this section has stimulated an awareness of and a feeling for the right to privacy. Indeed, it is this awareness from which, as witnessed by the Brandeis article, the right to privacy was conceived and upon which it will mature. Courts and legislatures respond or react to public concerns and, in that sense, it is we who will shape the future of the right to privacy.

CHAPTER IV: THE ECONOMICS OF SECURITY

INTRODUCTION AND OVERVIEW

The security decision is necessarily an organization and installation dependent problem. There is no universal solution to the question:

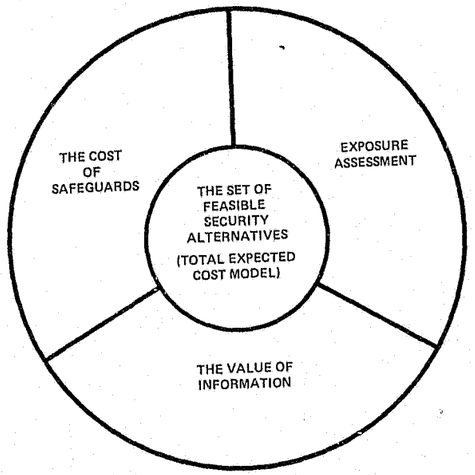
How do you determine the most cost-effective mix of security safeguards to address my organization's information privacy and security problem?

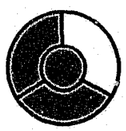
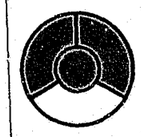
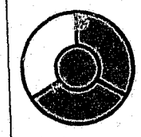
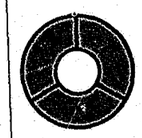
Clearly, however, any attempt to analyze carefully the problem will result in at least a better understanding of your organization's vulnerability and a rational basis for choosing (or not choosing) a given set of technological and administrative safeguards to address the problem.

The security problem in your organization can probably be broken down into the following three components:

- What and where are the information exposure possibilities in the organization?
- What is the value of information in your systems?
- What security safeguards are available, how effective are they and at what cost?

The illustration below depicts the components of the security decision. In the following material, each component will be treated to establish a rational framework for selecting a cost effective mix of administrative and technological safeguards.



ELEMENTS	QUESTIONS	METHODOLOGY
	What and where are the exposures confronting information in the organization?	1. Categorize exposures. 2. Identify specific access vulnerabilities and estimate exposure probabilities. 3. Document exposure areas, vulnerabilities and probabilities.
	What is the value of the organization's information resources?	1. Itemize the information resources of the organization. 2. Estimate the value of the information. 3. Document the value of the organization's information.
	What safeguards are available and what are their corresponding costs?	1. Research available safeguards and list those appropriate with corresponding conversion and operational costs. 2. Estimate the probability of given safeguards failing.
	What is the most cost effective mix of security safeguards to address the organization's privacy and information security problem?	1. Apply total expected cost model.

The specific methodology that will be used to generate the set of feasible security alternatives is summarized below.

First, this chapter will address the first three components of the security decision; namely, exposure assessment, information valuation and safeguard cost identification. Specifically, it will deal with your data gathering requirements and describe the tools that can be used to gather this data.

Next, a model will be described which was designed to develop a set of feasible security alternatives. The model is based on the total expected cost of security considering your organization's exposures, available safeguards and the value of information. The constraints on the model include your budget, the availability of the data and the state of the art in security technology.

As an indication of what is to follow, it is appropriate to consider briefly the approach and intent of the Total Expected Cost Model in this overview.

The model attempts to determine the most cost-effective combination of administrative and technological safeguards. This is accomplished by summing the cost of each security system and the expected loss associated with each system. The alternative with minimum total expected cost for a given data processing center is selected as the "best" security system for the center.

A security system is defined as a collection of 0, 1, 2, or more safeguards. For example, if there are only two safeguards available for securing a data processing center, call them Safeguard A and Safeguard B, then you have four possible security systems to choose from. These are:

- Use neither A nor B; i.e., employ no safeguards.
- Use Safeguard A only.
- Use Safeguard B only.
- Use both A and B.

The total expected cost of security has two major components. The first is the cost of installing and operating the safeguards. This is a real, out-of-pocket cost which can be determined relatively easily. The second is the cost (or loss) associated with the exposure of information being secured by the system. This loss due to exposure is not easily determined and must be based on estimates of the value of the resource and the probability someone will attempt to expose it and be successful. It is not a real cost in the sense that you know for certain that you will have to pay it, but rather an expected cost based upon two probabilities — the probability someone wants to expose information and the probability the safeguard(s) being used to protect if fails to formulate the problem, let:

X_k = cost ($/year) to install and operate the safeguards comprising security system k.

Y_k = expected loss ($/year) due to exposure if security system k is used.

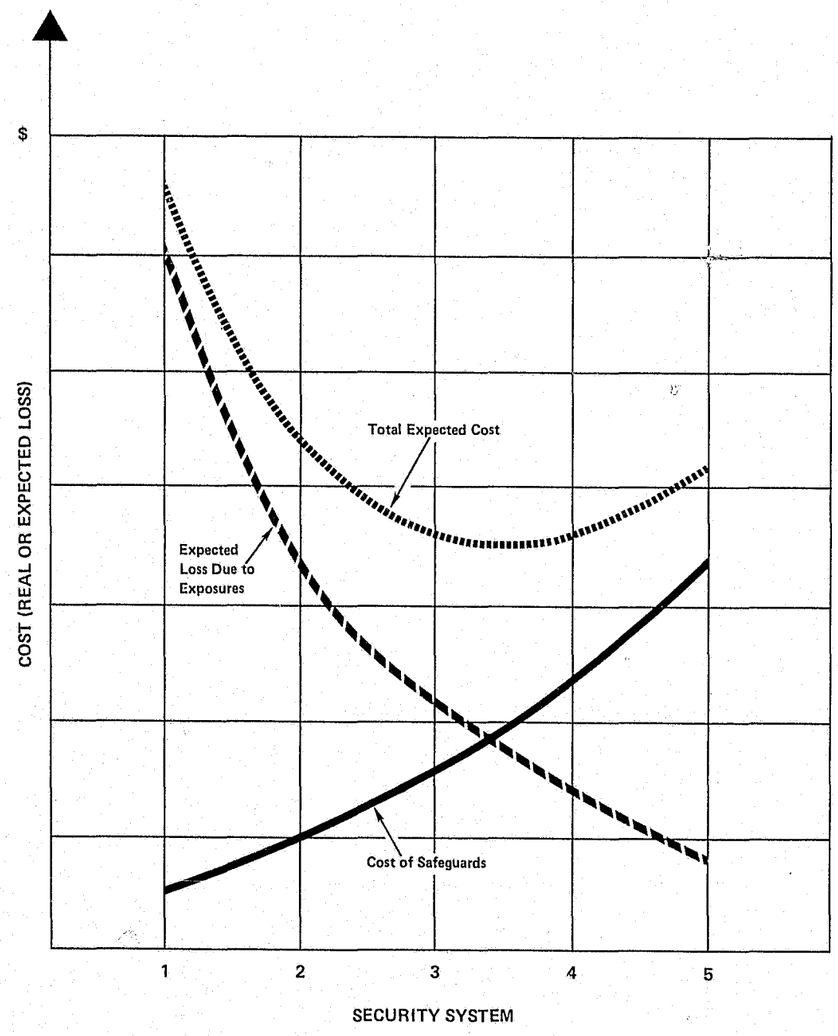
TEC_k = total expected cost ($/year) in using security system k.

Then, $TEC_k = X_k + Y_k$.

The cost versus loss trade off becomes clear through use of the formula. With few effective safeguards and a resultant low cost in providing security, the expected loss due to exposure will be high. On the other hand, an increase in the number of effective safeguards employed will increase the cost of providing security and reduce the expected loss due to exposure.

The problem is to find the correct balance of the two costs, X_k and Y_k (i.e., the security system k which minimizes the total expected cost).

The solution to this problem is illustrated graphically below.



TOTAL EXPECTED COST CURVE

In this example, two cost curves, X_k and Y_k, are plotted. The total expected cost curve is simply the sum of the values comprising X_k and Y_k. Your total expected cost is minimized if security system $k = 3$ is chosen.

The following pages will now describe what data is required and how this data can be used to generate **your** total expected cost curve.

METHODS OF DATA COLLECTION

To utilize the Total Expected Cost (TEC) Model approach to determine the most cost-effective mix of safeguards, you must determine the probability of information exposure, the value of the information in your systems and the types and costs of safeguards available to protect your information.

EXPOSURE ASSESSMENT

For the purpose of this data collection methodology your organization's information exposures should be defined as the accidental and/or intentional **alteration, destruction or disclosure** of information. In order to assess the exposures within your organization you should identify:

- The location of information in the information processing framework.
- The physical form of information. (Is it printed output, disk packs, tape reels, etc.?)
- The relationship between information in its physical form and location and the other information system resources.

The location, form and relationships of information to other resources are treated separately below to provide understanding of the methodology.

LOCATION OF INFORMATION

The information processing framework has been broken down into the following steps. These steps should be used to locate information in the various stages of processing.

- **Data Gathering.** The manual creation and transportation of data.
- **Data Transmission.** The manual movement of source documents to the input area in which source documents are converted to machine readable form.
- **Data Conversion.** The physical conversion of manual source documents to machine readable form.
- **Data Communication-Input.** The transmission of machine readable data (e.g., TP, messenger, mail, etc.).
- **Data Receipt.** The receipt of data via communications facilities and stored awaiting processing.
- **Data Processing.** The execution of application programs to perform intended computations and preparation of the result of the computations.
- **Output Preparation.** The preparation of output media for dissemination to users including tapes, cards, disk, drum, and paper.
- **Data Movement.** The manual movement of computer produced output, in various media form, to the output area to await user pick-up.
- **Data Communication-Output.** The transmission of output to the user, (e.g., TP, messenger, mail).
- **Data Usage.** The use of data by the recipient, including the storage or location of it while it is being used.
- **Data Disposition.** The disposition of data after the period of usage including the methods and locations of storage, length of time for storage and final disposal, as appropriate.

FORM OF INFORMATION

In order to reduce the potential exposure of information you must also identify its form at the various steps in the processing framework. Consider the following classifications:

- **Human Readable Media.** This classification includes information which can be read and understood by personnel including source documents, printed listings, systems and program documentation, interpreted (printed) punched cards and output reports.
- **Computer and Equipment Readable Media.** This classification includes information which can be read and interpreted by computer and other equipment including information located in main memory or on disk packs, magnetic drums, magnetic tapes, punched cards, microfilm and microfiche.

RELATIONSHIPS BETWEEN INFORMATION AND OTHER INFORMATION SYSTEM RESOURCES

The exposure assessment depends not only on the form or media of the information and the location of it in the processing cycle but also on the relationships of it to the other processing resources within your organization.

For the purpose of this methodology "other resources" have been classified as follows:

- **Personnel Resources.**

  a. EDP management
  b. Data center management
  c. Computer operations personnel
  d. I/O control personnel
  e. Clerical personnel
  f. Systems and programming management
  g. Systems analysts
  h. Programmers
  i. Software specialists
  j. User personnel

- **Physical Site Components.**

  a. Power supply
  b. Heating, air conditioning, humidity control equipment
  c. Walls, windows, doors, floors, ceiling
  d. Lighting, water supply
  e. Fire prevention/retardation equipment

- **Support Equipment.**

  a. Storage vaults
  b. Storage cabinets (forms, disk, tape, card)
  c. Utility carts, tables, scheduling boards, work flow control materials, and equipment status boards
  d. Bursting, decollating and shredding equipment
  e. Microfilm/microfiche and copying equipment

- **Computer Equipment.**

  a. Local
     — Terminals
     — Central processors
     — Consoles
     — Drum, disk, tape drives
     — Card readers, punches, printers, paper tape readers/punches
  b. Remote
     — Printers, card readers, paper tape readers/punches
     — Video displays
     — Consoles
     — Terminals

- **Communication Equipment.**

  a. Modems
  b. Processors
  c. Line junction boxes
  d. Lines

- **Software.**

  a. Computer operating programs
  b. File management and resource accounting programs
  c. Compilers, utility programs
  d. Communication control programs
  e. Program access control programs
  f. Application programs

- **Access Control Equipment.**

  a. Badge readers
  b. Access control computer
  c. Television cameras
  d. Television screen monitors

RELATIONSHIPS BETWEEN INFORMATION IN THE INFORMATION SYSTEM FRAMEWORK AND OTHER RESOURCES

		INFORMATION SYSTEM FRAMEWORK										
		DATA GATHERING	DATA TRANSMISSION	DATA CONVERSION	DATA COMMUNICATION-INPUT	DATA RECEIPT	DATA PROCESSING	OUTPUT PREPARATION	DATA MOVEMENT	DATA COMMUNICATION-OUTPUT	DATA USAGE	DATA DISPOSITION
FORM OF INFORMATION A = COMPUTER INTERPRETABLE B = HUMAN READABLE		B SOURCE DOCUMENTS	B SOURCE DOCUMENTS	A,B SOURCE DOCUMENTS CARDS, TAPE	A,B CARDS, TAP DISK DRUM	A TAPE DISK DRUM	A MAIN STORAGE	A,B CARD, TAPE DISK, DRUM PAPER REPORTS	A,B TAPE PAPER REPORTS CARDS	A,B CARDS, TAPE DISK PAPER REPORTS PUNCH-TAPE	B PAPER REPORTS FICHE MICROFILM	A,B DISK, TAPE PAPER REPORTS FICHE MICROFILM PUNCH-TAPE
RESOURCES	PERSONNEL	●	●	●	●	●	●	●	●	●	●	●
	PHYSICAL SITE COMPONENTS	●	●	●	●	●	●	●	●	●	●	●
	SUPPORT EQUIPMENT			●					●		●	●
	COMPUTER EQUIPMENT LOCAL AND REMOTE	●			●	●	●	●		●		
	COMMUNICATION EQUIPMENT				●	●				●		
	SOFTWARE				●	●	●	●		●		
	ACCESS CONTROL EQUIPMENT						●	●	●		●	●

The chart above illustrates the form of information in each activity within the information system framework. The chart also shows the noninformation resources which operate on or with information at each step in the framework.

Through the use of this chart or a similar display technique, you can isolate the location of information in human and computer readable form or media within the specific activities of the information system framework.

The next step in order to assess the exposure of your organization's information to accidental and/or intentional **alteration, destruction** or **disclosure** is to estimate the probability that someone will attempt to expose the information and be successful.

Generally stated, the probability of exposure depends on the number of personnel and other information system resources granted access to information. Additionally, the degree of access (e.g., restricted, full) will also play a role in determining exposure probability.

EXPOSURE PROBABILITY

An understanding of the number of personnel and other resources having access to information is vital to estimating exposure probability. You must also understand **how** personnel and other resources can access information. To assist in this understanding various **access routes** have been defined to illustrate how information can be accessed.

Four primary access routes have been defined and include physical access to information through a remote processing site or through a local processing site:

- **To Remote Processing Equipment.**

  The intruder may gain entry to a remote processing site and access information in its various forms or media either directly through the processing equipment or through the operating system or some programming interface.

- **To Local Processing Equipment.**

  The intruder may gain entry to the local data processing center the access information either directly through the processing equipment or again through the operating system or some programming interface.

- **Computer Media Information.**

  The intruder may gain physical entry to the local processing site and access computer media information (i.e., disk packs, tape reels, etc.)

- **Human Readable Media.**

  This route includes physical entry to the processing facility and access to human readable media such as printed cards, output reports, program and system documentation.

You will note that each of the four main access routes include entry to the remote or local physical site. The following chart illustrates the four primary access routes and provides for estimating the **rate** of attempted access through the various routes and subroutes. The chart contains forty-eight individual access routes. The first twelve routes are explained as follows. The specific subroutes within each of the primary routes 2, 3, and 4 are derived in the same manner as the subroutes illustrated for primary route #1 and therefore are not shown.

Access Routes and Sub-Routes

Primary Route #1	**Sub-Route #'s**
Access to human readable or computer media information through the remote site equipment, operating system and/or programming.	**1-4 Disclosure**
	1-2 Insider (Inside Personnel)
	1. Accidental
	2. Intentional
	3-4 Outsider (Outside Personnel)
	3. Accidential
	4. Intentional
	5-8 Alteration
	5-6 Insider
	5. Accidental
	6. Intentional
	7-8 Outsider
	7. Accidental
	8. Intentional
	9-12 Destruction
	9-10 Insider
	9. Accidental
	10. Intentional
	11-12 Outsider
	11. Accidental
	12. Intentional

EXPOSURE PROBABILITY

METHODOLOGY FOR DETERMINING LIKELIHOOD OF ATTEMPTED ACCESS TO INFORMATION

TIME FRAME FOR THE PROBABILITY _____ TITLE OF INFORMATION SYSTEM BEING ASSESSED _____

RESULTS

ROUTE OF ATTEMPTED ACCESS (REMOTE PROCESSING SITE)	DISCLOSURE				ALTERATION				DESTRUCTION			
	INSIDER		OUTSIDER		INSIDER		OUTSIDER		INSIDER		OUTSIDER	
	ACCIDENTAL RATE	INTENTIONAL RATE	ACCIDENTAL RATE	INTENTIONAL RATE	ACCIDENTAL RATE	INTENTIONAL RATE	ACCIDENTAL RATE	INTENTIONAL RATE	ACCIDENTAL RATE	INTENTIONAL RATE	ACCIDENTAL RATE	INTENTIONAL RATE
1. PHYSICAL SITE												
REMOTE COMPUTER EQUIPMENT												
OPERATING SYSTEM												
PROGRAMMING												
HUMAN READABLE OR COMPUTER MEDIA INFORMATION												
2. PHYSICAL SITE (LOCAL PROCESSING SITE)												
LOCAL COMPUTER EQUIPMENT												
OPERATING SYSTEM												
PROGRAMMING												
HUMAN READABLE OR COMPUTER MEDIA INFORMATION												
3. PHYSICAL SITE												
COMPUTER MEDIA INFORMATION												
4. PHYSICAL SITE												
HUMAN READABLE INFORMATION												

CHOICES		NUMBER OF ATTEMPTS PER TIME FRAME	RATES AT ATTEMPTED ACCESS 1 YEAR	3 YEARS	5 YEARS
(N)	NEVER	0	0	0	0
(S)	SELDOM	1-3	2	2/3	2/5
(O)	OFTEN	4-8	6	2	6/5

INSTRUCTIONS:

(1) PICK TIME FRAME (1, 3 OR 5 YEARS).
(2) ESTIMATE NUMBER OF ATTEMPTS (YOU HAVE THREE CHOICES: NEVER (N), SELDOM (S), AND OFTEN (O). SEE ABOVE FOR DEFINITION OF THE CHOICES AND THE RESPECTIVE RATES OF ATTEMPTED ACCESS,).

To apply the methodology shown in the chart you should:

Step 1. Determine the time frame within which you will estimate the probability — normally from one to five years.

Step 2. Estimate the **rate** of access for each of the 48 access **routes**. To assist you the rates have been categorized three ways:

(N) — **Never** — access not probable
(S) — **Seldom** — access likely 1 to 3 times within the estimating time frame
(O) — **Often** — access likely 4 to 8 times within the estimating time frame

Step 3. Apply the estimated rates of acces for applicable routes to the Total Expected Cost Model.

An example of how this chart is used is shown in Appendix G.

INFORMATION VALUATION

The determination of information value contains elements of opinion and subjectivity and therefore is relative to your organization. The value you place on your information will necessarily reflect the following perspectives:

- Value to you, the custodian of the information.
- Value to the subject about whom the information is maintained.
- Value to an intruder desiring to obtain information.

The methodology for determining information value necessarily focuses on your perspective as the custodian of the information. Where it is practical to identify subject and intruder value you should do so, because there consideration is useful to assess the value of information to you and the risk of its exposure.

The chart shown below illustrates the methodology for assessing information value. You will note that value is expressed two ways:

- **Dollar Value.** Dollar value is assessed through quantitative estimates of costs and/or out-of-pocket expense.
- **Utility Value.** Utility value is expressed subjectively and converted to dollars based on the impact or importance of the utility factor to your organization (a utility factor dollar conversion scale is included on the chart).

Scale for converting Utility Value to dollars based on impact or importance of the utility factor to the organization.

5 - Maximum	=	$100,000
4 - High	=	$ 75,000
3 - Medium	=	$ 50,000
2 - Some	=	$ 25,000
1 - Little	=	$ 1,000

VALUE CALCULATION METHOD

DOLLAR VALUE ILLUSTRATION

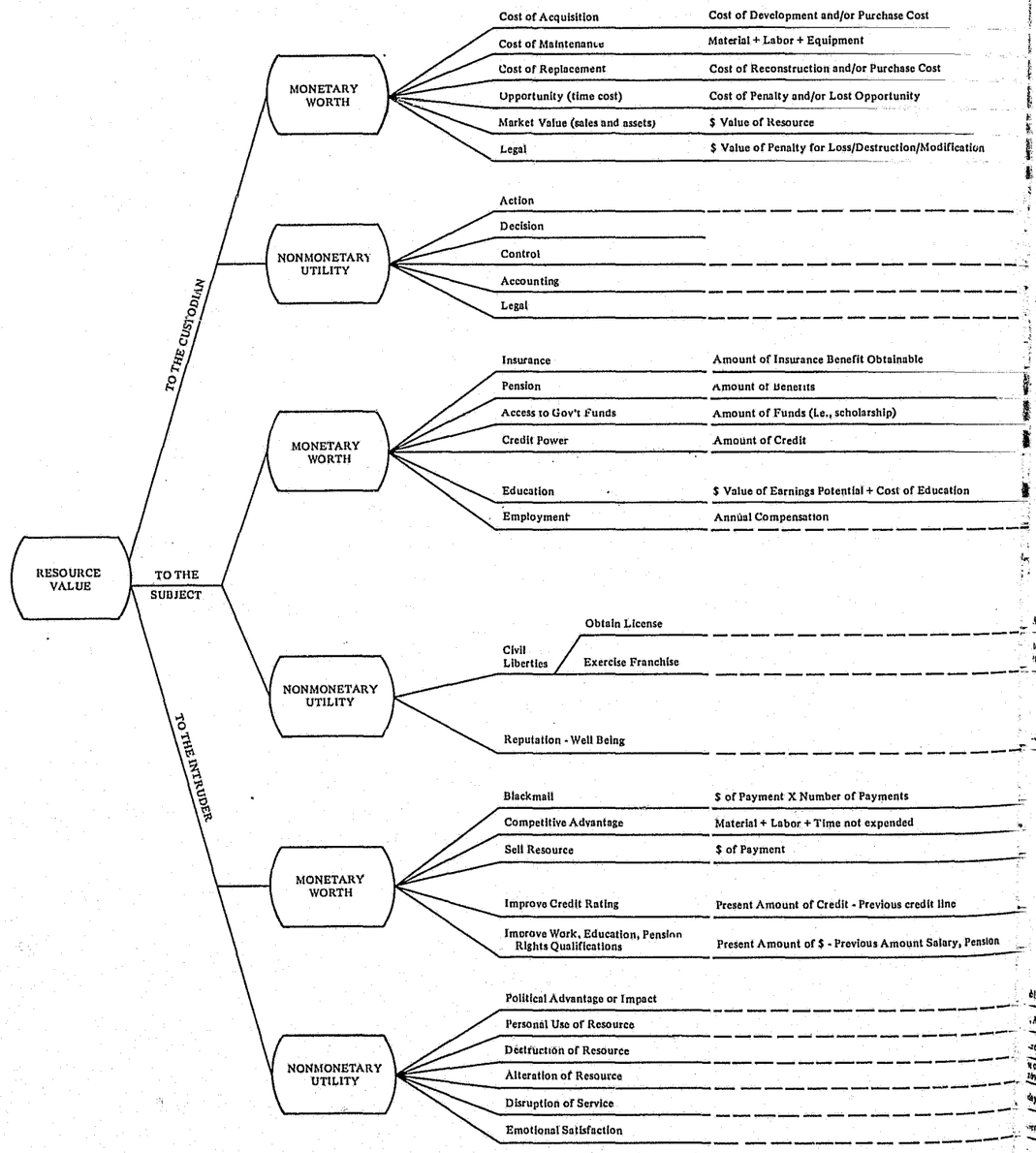


EXHIBIT VI

ILLUSTRATION OF UTILITY VALUE TOTAL

	CUSTODIAN		SUBJECT		INTRUDER				
	$VALUE	UTILITY	$ VALUE	UTILITY	$ VALUE	UTILITY	$ VALUE TOTAL	UTILITY TOTAL	OVERALL TOTAL
	$								
	$								
	$								
	$								
	$								
	$								
of Inability to Act or Mission									
of Inability to Make Decisions		$					$		
of Loss of Control erations (waste)									
of Inability to for Operations									
of Loss of Authorization									
								$	
			$						
			$						
			$						
			$						
			$						
			$						
							$		
Activity Authorization									
to Regulate st Action			$						
, Health								$	
			$						
			$						
			$						
							$		
			$				$		
Ability to Cause									
Advantage; Convenience							$		
racy									
of Altered Resource: irements									
day									
rage									
								$	
							$	+	= $

To use the methodology shown you should first identify the information to be valued (i.e., an information system, master and/or transaction file, output reports, etc.), then proceed from left to right on the exhibit assessing value from each of the perspectives.

SAFEGUARD AND COST IDENTIFICATION

After you have assessed the exposure probability of the information in your organization and identified the value of the information, the types and costs of safeguards available must be determined. Safeguards have been classified two ways:

- Technological
- General Management

With each type of safeguard there are two associated costs; the direct cost or the cost of purchase or lease of given safeguards, and the indirect or operating costs associated with the safeguards. Safeguards are further classified as follows:

- **Technological Safeguards.**
  - — Physical Plant Access Controls
  - — Physical Plant Disposal Controls
  - — Software Controls
  - — Teleprocessing Controls

- **General Management Safeguards.**
  - — General Security Education
  - — Organization for Security
  - — Policy Development
  - — Systems Assurance

The chart on the next two pages illustrates some of the safeguard types and associated cost considerations. You should investigate the types and costs of safeguards and select those appropriate for your organization. When the selected safeguard combinations are included in the Total Expected Cost (TEC) Model, it will become apparent that certain of the combinations are more cost effective than others.

SECURITY SAFEGUARD COST CONSIDERATIONS

SAFEGUARD TYPES / COST CONSIDERATIONS			ASSOCIATED CONVERSION COST CONSIDERATIONS	ASSOCIATED OPERATION COST CONSIDERATIONS	
				DIRECT	INDIRECT
TECHNOLOGY	PHYSICAL PLANT ACCESS CONTROLS	1. Use of key or combination lock to gain access	Distribute keys and combinations to authorized people Develop distribution procedures Education		On-going Education
		2. Sign-in/Sign-out with guard or receptionist checking identification card	Develop sign-in/sign-out procedure Develop identification procedure by shift and skill type Hire guard or receptionist Identification media creation and distribution Develop control procedures for lost identification media Develop procedure to control file movement Education	Guard or receptionist salary Maintenance	Audit
		3. Automated access control system with magnetic badge	Badge creation and distribution costs Install system (e.g., electrical and mechanical work, physical planning, software costs, etc.) Develop violation action procedure Education	Equipment rental Maintenance	Audit
		4. Automatic access control system with magnetic badge and guard	Same as in (3) Hire guard	Same as in (3) Guard salary	Audit
		5. System as in (4) with surveillance and alarm equipment	Same as in (4)	Same as in (4)	Audit
	PHYSICAL PLANT DISPOSAL CONTROLS	1. No disposal controls	None	None	None
		2. Compactors	Develop procedure for disposal of confidential obsolete information and trash Equipment installation	Equipment cost Maintenance	Audit
		3. Shredders	Same as in (2)	Same as in (2)	Same as in (2)
		4. Information liquefying process	Same as in (3)	Same as in (3)	Same as in (3)
	SOFTWARE	1. No software security	Develop control procedures for changes to vendor supplied software, application programs, testing sensitive applications, operating systems documentation, and application program documentation	Staff for enforcement and execution	Technology research Audit
		2. Software with FETCH Protect	Same as in (1) Install FETCH Protect software (SYSGEN, test & implement) Write attempted integrity violation procedure Develop procedures for software security documentation control Education for software, operations staff & users Application program change costs	Analyze & remedy attempted violations Computer overhead Software maintenance	Same as in (1) On-going education for users & staff
		3. Software with FETCH & Integrity features	Same as in (2)	Same as in (2)	Same as in (2)
		4. Software as in (3) with logging functions	Same as in (3) Develop interface with operating system subsystems	Same as in (3)	Same as in (3)
		5. Software as in (4) with data set authorization functions	Same as in (4) Develop information classification guidelines Develop profile definition procedure Define profiles Develop codeword distribution and change procedures	Same as in (4) Real time administration	Same as in (4)
		6. Software with (5) and field & record level capability	Same as in (5)	Same as in (5)	Same as in (5)
		7. Software with (6) & over write capabilities	Same as in (6) Develop overwrite procedures	Same as in (6)	Same as in (6)

CHART CONTINUED ON NEXT PAGE

SECURITY SAFEGUARD COST CONSIDERATIONS

SAFEGUARD TYPES / COST CONSIDERATIONS			ASSOCIATED CONVERSION COST CONSIDERATIONS	ASSOCIATED OPERATION COST CONSIDERATIONS	
				DIRECT	INDIRECT
TECHNOLOGY	TELEPROCESSING CONTROLS	1. No TP controls	None	None	Technology research
		2. Terminal Location Controls	Location control devices (e.g., locks on doors, guards, etc.) Secure communication line junction points & modems Develop physical access control procedures	Staff for enforcement &execution Maintenance	Technology research Audit
		3. Terminal Use Controls as well as (2)	Same as in (2) Hardware features (e.g., badge reader, hardwired passwords, etc.) Develop procedures for use of hardware functions	Same as in (2) Rental Costs Overhead	Same as in (2)
		4. Software Controls as well as (3)	Same as in (3) Install software (SYSGEN, test, implement) Develop TP Control program interface Develop procedures for use of TP software functions	Same as in (3) Software maintenance	Same as in (3)
		5. Line controls in addition to (4)	Installation costs (encryption, cable shielding, etc.)	Same as in (4) Additional line costs	Same as in (4)
GENERAL MANAGEMENT	GENERAL EDUCATION	1. Problem definition and code of conduct	Program development Media communication costs		On-going administration
		2. Executive Programs (organization considerations, policy considerations, implementation approach, etc.)	Same as in (1)		Same
		3. General Administrative Considerations (work flow controls, personnel practices, etc.)	Same as in (2)		Same
		4. Security in Systems Design	Same as in (3)		Same
	ORGANIZE FOR SECURITY		Develop organization structure Write job descriptions Establish qualification criteria Hiring and Staffing costs Training costs Develop Budget		On-going administration costs
	POLICY DEVELOPMENT		Write policies Communicate Policy	Administration & enforcement	Administration Audit
	SYSTEMS ASSURANCE		Develop security guidelines for systems design and programming		Audit

METHOD FOR DETERMINING THE BEST SECURITY SYSTEM

Different security systems, or levels of security, can be achieved by using different combinations of safeguards. The problem, therefore, is to find the "best" combination of safeguards to secure the resources of a given center. The alternative security systems range from employing no security devices to using a number of safeguards (for example, hardware, software, and administrative practices.) The method used to find the best security system involves determining the total expected cost (TEC_k) for each alternative, k. The alternative with minimum total expected cost for a given data processing center is selected as the best security system for the center.

The method is illustrated with an example using real data and based upon a real situation, the protection of birth records within the State of Illinois which are maintained and processed by the Office of Vital Records and the MID.

The exposure access route describes the type of exposure, how and by whom it can be performed, and the form in which the information can be obtained. Using the methodology previously described, an estimate of the average number of attempts per year to expose birth records via the forty-eight possible exposure access routes was performed, assuming a system of safeguards presently employed by the MID and the Office of Vital Records. Five of the exposure access routes (numbers 2, 5, 6, 26, 38) were found to be vulnerable, that is, it was estimated that the average number of attempts per year to expose birth records via these routes would be greater than zero. It was predicted that no one could or would ever attempt to expose birth records by way of the other routes, that is, they are not routes which are vulnerable to exposure.

To estimate the value of birth records, if exposed, officials at the Office of Vital Records for the State of Illinois used the method of determining resource value described earlier. The estimates for the value of birth records and the average number of attempts per year to expose them are given in the table below. A detailed explanation of the methodology used to obtain these estimates is given in Appendix G.

TABLE 1

EXPOSURE ACCESS ROUTE NUMBER	EXPOSURE ACCESS ROUTE	VALUE OF RESOURCE ($ PER EXPOSURE)	AVERAGE NO. OF ATTEMPTED EXPOSURES PER YEAR	EXPECTED LOSS EXPOSURE ACCESS RTE. (PROD. OF PREV. 2 COL.
2	Intentional disclosure of human readable or computer media information via remote equipment by an insider.	$250,000	0.4	$100,000
5	Accidental alteration of human readable or computer media information via remote equipment by an insider.	775,000	1.2	930,000
6	Intentional alteration of human readable or computer media information via remote equipment by an insider.	775,000	0.4	310,000
26	Intentional disclosure of computer media information at the local site by an insider.	250,000	0.4	100,000
38	Intentional disclosure of human readable information at the local site by an insider.	250,000	0.4	100,000

This information is now used to determine the best security system for the one resource, birth records. To maintain a manageable example, it is assumed that this resource is the only one that the MID and the Office of Vital Records is interested in protecting from exposure. Clearly, in a real situation there are many resources worth protecting. However, the method that follows for determining the best security system would remain the same for more than one resource, only the number of calculations would increase.

After identifying all the exposure access routes through which it is estimated information will be exposed if no new safeguards are employed, you can limit your investigation of safeguards to those which protect these routes. In this case, five safeguards have been identified. They are given in the table shown below, which also includes the exposure access routes these safeguards protect and an estimate of the probability the safeguard fails, given an attempt is made to expose a resource it protects.

TABLE 2

SAFEGUARD NO.	EXPOSURE ACCESS ROUTES PROTECTED	SAFEGUARD TYPE	PROBABILITY SAFEGUARD FAILS, GIVEN AN ATTEMPT IS MADE TO EXPOSE RESOURCE
0	none	No new safeguards.	1.00
1	2, 6	Audit trail at remote location (software).	0.05
2	5	Verification checking at remote location (hardware and personnel).	0.02
3	2, 6	Authorization checking at remote location (software).	0.00
4	26, 38	Exist control at local site (personnel).	0.02
5	26, 38	Surveillance at site (hardware & personnel).	0.30

The following table shows the implementation and operating costs for the safeguards being considered and a description of how these costs were obtained. In all cases where personnel are required, overhead (indirect) expenses are assumed to be 50% of salaries or wages.

TABLE 3

SAFEGUARD NO.	DESCRIPTION OF SAFEGUARD	COSTS	
		IMPLEMENTATION ($)	OPERATING ($/YEAR)
0	No new safeguards	0	0
1	Clerk works ½-time for one shift; salary, $8,000/year. Operating cost = ½(8,000 + 4,000).	$10,000	$ 6,000
2	Verifier works 3/4 the time of the operator; operator works ½-time; salary, $8,000/year; hardware rental 200/month. Operating cost = 3/4 (½(8,000 + 4,000)) + 12(200).	2,000	6,900
3	Software rental $3,000/month.	50,000	36,000
4	One guard on each of three shifts, seven days/week; five guards required in total; salary $8,000/year. Operating cost = 5(8,000 + 4,000).	6,000	60,000
5	Same as safeguard 4, with the addition of $10,000 worth of equipment – a one-time purchase.	16,000	60,000

In both Tables 2 and 3, above, safeguard number 0 is used to indicate the alternative of no new security devices.

The following table shows the probability a safeguard fails to prevent exposure of birth records, given an attempt is made to expose them by way of the vulnerable exposure access routes. This table is based upon the information given in Table 2 and is presented in this form to show more clearly the relationship between the safeguards and the vulnerable exposure access routes of this example. When no new safeguards are employed, the probability of failure is 1.00 for all vulnerable routes. In other words, if someone attempts to expose birth records via one of the vulnerable exposure access routes, the chance of success is 100%. However, when safeguard 1 is employed, the probability this safeguard fails to prevent exposure is .05 for routes 2 and 6, and 1.00 for routes 5, 26 and 38. This means that if someone attempts to expose birth records via routes 2 and 6, the chance of success is 5%. But safeguard 1 does not protect against exposure by way of routes 5, 26, or 38, hence the chance of success is 100% for these routes.

TABLE 4

SAFEGUARD NO.	EXPOSURE ACCESS ROUTE NUMBER				
	2	5	6	26	38
0	1.00	1.00	1.00	1.00	1.00
1	.05	1.00	.05	1.00	1.00
2	1.00	.02	1.00	1.00	1.00
3	0.00	1.00	0.00	1.00	1.00
4	1.00	1.00	1.00	.02	.02
5	1.00	1.00	1.00	.03	.03

Table 5 gives all the possible security systems, k, for this example; the safeguards which comprise them; X_k; Y_k; and TEC_k. The TEC_k are compared on a one-year basis. A very slight modification of the method, using discounted future expenses, is presented in Appendix H, where a five-year planning period is assumed. Table 5 is also redone in Appendix H, using a five-year planning period.

TABLE 5

SECURITY SYSTEM k	SAFEGUARDS COMPRISING k	XI_k ($)	XO_k ($)	X_k ($)	Y_k ($)	TEC_k ($)
0	0	0	0	0	1,540,000	1,540,000
1	1	10,000	6,000	16,000	1,150,000	
2	2	2,000	6,900	8,900	628,600	637,500
1	3	50,000	36,000	86,000	1,130,000	
4	4	6,000	60,000	66,000	1,342,000	
5	5	16,000	60,000	76,000	1,400,000	
6	1,2	12,000	12,900	24,900	239,100	264,000
7	1,3					
8	1,4	16,000	66,000	82,000	954,500	
9	1,5	26,000	66,000	92,000	1,010,500	
10	2,3	52,000	42,900	94,900	218,600	
11	2,4	8,000	66,900	74,900	432,600	
12	2,5	18,000	66,900	84,900	488,600	
13	3,4	56,000	96,000	152,000	934,000	
14	3,5	66,000	96,000	162,000	990,000	
15	4,5	16,000	60,000	76,000	1,341,200	
16	1,2,3					
17	1,2,4	18,000	72,900	90,900	43,100	134,000
18	1,2,5	28,000	72,900	100,900	99,100	
19	1,3,4					
20	1,3,5					
21	1,4,5	26,000	66,000	92,000	951,700	
22	2,3,4	58,000	102,900	160,900	22,600	183,500
23	2,3,5	68,000	102,900	170,900	78,600	
24	2,4,5	18,000	66,900	84,000	429,800	
25	3,4,5	66,000	96,000	162,000	931,200	
26	1,2,3,4					
27	1,2,3,5					
28	1,2,4,5	28,000	72,900	100,000	40,300	141,200
29	1,3,4,5					
30	2,3,4,5	68,000	102,900	170,900	19,800	190,700
31	1,2,3,4,5					

The costs for security systems 7, 16, 19, 20, 26, 27, 29 and 31 have not been calculated because each of these systems contains safeguards 1 and 3. Safeguard 1 does not contribute anything except additional cost to such systems. It does not provide additional security for the exposure access routes 2 and 6 which it protects because safeguard 3 provides "complete" security for these routes, that is, if someone were to attempt to expose birth records by way of route 2 or 6, the chance of success would be 0.00 if safeguard 3 was being used. Therefore, security systems containing safeguards 1 and 3 are redundant. In some cases Table 5 does not show the value for TEC_k where X_k and Y_k have been calculated. Such systems are dominated by other systems in this example and, therefore, would never be picked as the best security system for this situation. For example, security system 1 is dominated by security system 2 because both the cost, X_1, and the expected loss, Y_1, for this system are greater than the cost, X_2, and expected loss, Y_2, for system 2. The method for obtaining the values in Table 5 is now described.

The basic model for finding the best combination of safeguards to secure the resources of a data processing center was given previously, namely,

$$TEC_k = X_k + Y_k$$

where

X_k = cost ($/year) to install and operate the safeguards comprising security system k.

Y_k = expected loss ($/year) due to exposure if security system k is used.

TEC_k = total expected cost ($/year) in using security system k.

The cost X_k consists of two components — implementation cost and operating cost. Implementation cost is defined as a one-time start-up cost associated with using the safeguards in security system k. This might include equipment, training, computer programming, etc.. The operating costs are the yearly expenses required to keep the safeguards in use, (e.g., salaries, rental of software or hardware.) To formulate the model then, let:

XI_k = cost ($) to implement the safeguards comprising security system k.

XO_k = cost ($/year) to operate the safeguards comprising security system k.

Then, in this example where the costs of alternative systems are being compared on a one-year basis,

$$X_k = XI_k + XO_k$$

These costs are found in Table 3, shown previously. It should be noted, however, that care must be taken in determining X_k, since the safeguards comprising some systems share costs.

The loss Y_k is found by summing, over all the vulnerable exposure access routes, the product of the expected loss due to estimated attempted exposures per year and the probability of success of these attempts. For this example, the expected losses were given in Table 1 and the probabilities of success of attempted exposures, that is, the probabilities safeguards fail, were given in Table 4.

Some sample calculations, on which Table 5 was based, follow:

TEC_0:

$X_0 = 0$. No new safeguards are employed; hence, there is no new cost in providing security.

$$Y_0 = 100{,}000(1.00) + 930{,}000(1.00) + 310{,}000(1.00) + 100{,}000(1.00) + 100{,}000(1.00)$$
$$= \$1{,}540{,}000$$

$$TEC_0 = X_0 + Y_0 + 0 + 1{,}540{,}000 = \$1{,}540{,}000$$

TEC_1:

$$X_1 = XI_1 + XO_1 = 10{,}000 + 6{,}000 = \$16{,}000.$$

$$Y_1 = 100{,}000(.05) + 930{,}000(1.00) + 310{,}000(.05) + 100{,}000(1.00) + 100{,}000(1.00)$$
$$= \$1{,}150{,}500$$

$$TEC_1 = X_1 + Y_1 = 16{,}000 + 1{,}150{,}500 = \$1{,}166{,}500$$

TEC_6:

$$X_6 = XI_6 + XO_6 = (10{,}000 + 2{,}000) + (6{,}000 + 6{,}900) = \$24{,}900$$

$$Y_6 = 100{,}000(.05)\ (1.00) + 930{,}000(1.00)\ (.02) + 310{,}000(.05)\ (1.00) + 100{,}000(1.00)\ (1.00) = \$239{,}100.$$

In security system 6 two safeguards, 1 and 2, are being employed. It is assumed the safeguards work independently of each other; hence the probability of a successful attempted exposure is the product of the probability the attempt will be successful against each safeguard.

$$TEC_6 = X_6 + Y_6 = 24{,}900 + 239{,}100 = \$264{,}000$$

TEC_{30}:

$X_{30} = XI_{30} + XO_{30}$ Note that safeguards 4 and 5 both use guards at the local site and these guards can perform both exit control and surveillance. Therefore, the operating cost and some implementation cost for these two safeguards are shared and must not be duplicated.

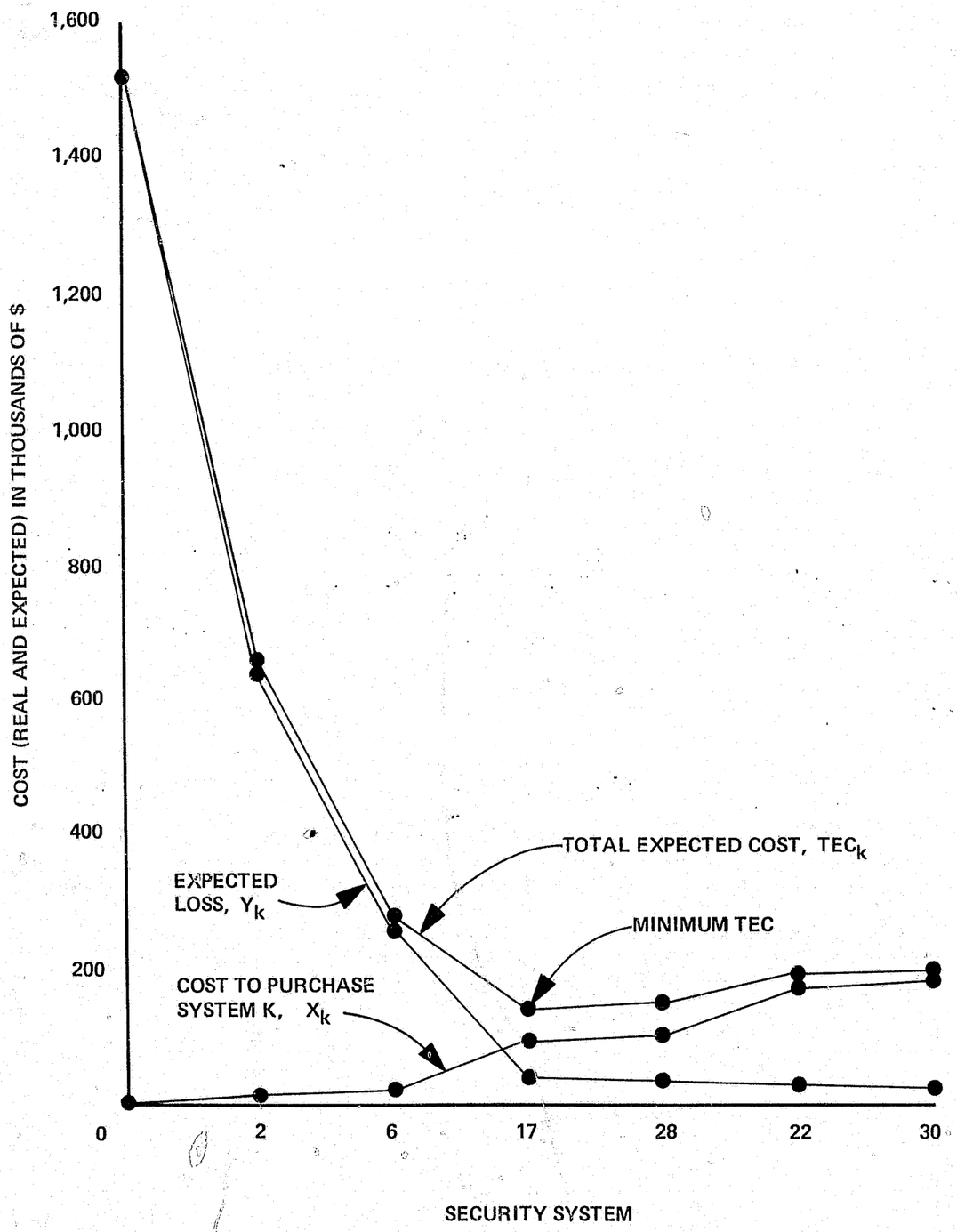
$$= (2{,}000 + 6{,}900) + (50{,}000 + 36{,}000) + (6{,}000 + 60{,}000) + (10{,}000 + 0) = \$170{,}900.$$

$$Y_{30} = 100{,}000(1.00)\ (.00)\ (1.00)\ (1.00) + 930{,}000(.02)\ (1.00)\ (1.00)\ (1.00) + 310{,}000(1.00)\ (.00)\ (1.00)\ (1.00) + 100{,}000(1.00)\ (1.00)\ (.02)\ (.30) + 100{,}000\ (1.00)\ (1.00)\ (.02)\ (.30) = \$19{,}800.$$

The product of probabilities here follows the same argument given in determining Y_6.

$$TEC_{30} = X_{30} + Y_{30} = 170{,}900 + 19{,}800 = \$190{,}700.$$

A graph of the results of Table 5 is given on the next page. Only the undominated security systems are shown on the graph. Security system 17, comprising safeguards 1, 2 and 4, is the system with minimum total expected cost. If you use minimum TEC as the only criterion for making the decision on the best level of security for the center, then you should select system 17. The graph shows that purchasing more security than provided by system 17, for example, security system 28 which employs safeguards 1, 2, 4, and 5, does not reduce expected loss from exposure enough to justify the additional cost, that is, TEC_{28} is greater than TEC_{17}.



This section has presented a method for determining the best level of security for a data processing center. Minimum total expected cost has been used as the criterion for selecting the "best" level of security. However, even if you find this criterion unsatisfactory, the methodology presented enables you to look at the problem objectively, to compare the various alternative security systems available and to narrow your choice to alternative systems by weeding out redundant and dominated alternatives. In most real situations there would be a constraint on the amount of money available to purchase safeguards. You can use the methodology of this section to help determine the best security system for your center while still adhering to a budget constraint. If a security budget constraint of $80,000 were imposed on the above example, it is clear that you should pick security system 6 over security systems 4, 5, 11, or 15. Nevertheless, you must apply good judgment and experience in making the security system decision. This methodology provides you with a framework for doing so. In the example, security system 6 costs less than one-third of the cost of security system 17, the "best" system. You might feel that the additional reduction in expected loss, due to exposure in going from system 6 to system 17, is not worth the additional real cost in safeguards, or you might choose to "take a chance." However, in comparing system 0 with systems 6 and 17, you are more likely to "take a chance" in using 6 over 17, than 0 over 6.

A complete development of the methodology presented in this section, as well as discussion of the assumptions which must be made in order to use it, appears in Appendix H.

SOME POTENTIAL PROBLEMS, REFINEMENTS AND POSITIVE SIDE EFFECTS

There are a number of refinements which can be made to the model and some problems associated with this approach to analyzing the economics of security. Namely,

- More work should be done to apply the concepts of Utility Theory to the value determination methodology.
- In very large and complex security systems, the number of calculations required to generate the model would prohibit manual calculation. Perhaps, after the model is further refined, an automated version can be developed.
- The assumptions which must be made to use the model (see Appendix H) may be inapplicable to certain types of environments.

Nevertheless, the application of the methodology described in this chapter to a few real information systems in the State of Illinois resulted in some positive side effects. It:

- Served as an excellent communication tool between the information technologist responsible for the design of a system and the user of the information system.
- Served to enlighten information system user management not only to security problems in automated systems but also to problems in manual systems.
- Reduced the purely emotional, event-driven response to security which typifies the attitude of many users, generators and operators of information systems.
- Caused a critical assessment of the information systems environment and promoted improved understanding of the type and number of actions necessary to improve the security of the environment.
- Illustrated the complexity of the information privacy and security problem and provided useful guidelines for "advancing the state-of-the-art".

It appears, then that this approach to analyzing security requirements can also provide a vehicle for communicating with and educating users, operators and generators of information systems to the need for creating a well-balanced security environment.

CHAPTER V: A SUMMARY OF GENERAL CONCLUSIONS AND RECOMMENDATIONS

This document has described the results of a multidisciplinary effort involving lawyers, computer specialists, statisticians, operations researchers, educators, administrators and management consultants. The results of the project clearly point to the need for action by both users of information systems and manufacturers of hardware and software systems.

The need for new technology which is more responsive to user requirements is apparent. Equally important, however, is the need for practical administrative and educational tools and guidelines which are necessary to support technology. The urgency of the situation is highlighted by the determined efforts of a number of federal and state legislators to introduce comprehensive privacy legislation. Project SAFE has attempted to define the requirements and considerations involved in establishing a viable balance between the technological, administrative and educational requirements consistent with the present day concept of an individual's right to privacy.

The following list summarizes the project's general conclusions and recommendations:

- **Conclusion:**
  There are precedents in constitutional law, common law and statutory law respecting an individual's right to privacy. There is a trend, however, to more clearly define this right at the state and federal level by introducing new legislation. The legislative recommendations of a joint effort involving the National Association for State Information Systems (NASIS), the Government Management Information Sciences users group (G-MIS) and Project SAFE are documented in a paper entitled "Records, Privacy and the Law — A Need for Legislative Action". **This effort was not funded by IBM.**

  Recommendation:
  The State of Illinois should investigate its present legislative posture regarding an individual's right to privacy.

- **Conclusion:**
  Policy statements related to the privacy of information and data security are necessary to indicate the concern and posture of the senior level executives within the state.

  Recommendation:
  All senior executives within the State of Illinois should explicitly state the information privacy and protection requirements for their jurisdiction in the form of written policy statements. The statements developed by Project SAFE may serve as a useful reference (see *Recommended Security Practices*).

- **Conclusion:**
  Substantive, enforceable procedures must be developed and supported by all levels of management involved in information system activities.

  Recommendation:
  Substantive procedures and job responsibilities must address:

  a. Personnel practices
  b. Work Flow Control
  c. Software Security Administration
  d. Terminal Access
  e. Systems Design
  f. Physical Plant Protection
  g. Contingency Planning
  h. Auditing Responsibilities

The procedures developed by Project SAFE should be adopted as appropriate (*Recommended Security Practices*).

- **Conclusion:**
  The concepts and safeguards relating to the privacy of information and data security should become an integral part of the training and education program of all generators, operators, and users of information systems.

  Recommendation:
  The videotape program of education developed by Project SAFE should be used and, if necessary, expanded by the information systems community within the State of illinois. In some instances, it may be advisable to develop workbooks or programmed instruction manuals to be used in conjunction with the videotape program (see Project SAFE *Session Leader's Guide*).

- **Conclusion:**
  Software security is a viable, necessary link in the information protection chain.

  Recommendation:
  A software security system should be designed with the concepts of Integrity, Isolation, Identification, Controlled Access and Surveillance in mind. Designers of a software security system should:

  a. Consider the performance of the software security system from the standpoints of functional certification, reliability and system degradation.
  b. Consider the changes to normal system support that are required to maintain system integrity.
  c. Assure that the degree of administrative procedural support required is minimal and enforceable.
  d. Assure that the impact on user applications is minimized and well-documented.
  e. Assure that the operating system and sub-systems are designed with security in mind and use a common security interface.
  f. Provide appropriate tools to facilitate software security system implementation and use.
  g. Use the functional capabilities defined herein as guidelines in the design of future software security systems.
  h. Provide the user with the flexibility to tailor a specific system to his requirements and budgetary constraints.
  i. Assure that proper tools and techniques are available to train all levels of the organization during conversion and on-going thereafter.

- **Conclusion:**
  Hardware security is a viable complement to a software security system. In fact, the effectiveness of a software security system is dependent on the reliability and serviceability of the hardware system.

  Recommendation:
  Manufacturers should investigate the feasibility of using hardware capability in lieu of software capability to support some security functions.

- **Conclusion:**
  Physical security is the "first line of defense" in any information systems environment.

  Recommendation:
  a. The feasibility of expanding the use of automated (people) access control systems to control file movement to and from state data centers should be investigated.
  b. The feasibility of a computer blockhouse to accommodate the computer hardware of the Agencies subject to the Governor should be investigated.
  c. The magnetic stripe badge used in the automated access control system developed by Project SAFE in conjunction with the Secretary of State should become the standard state ID.

Although these conclusions and recommendations are specifically aimed at the State of Illinois and manufacturers of hardware and software systems, the products, tools, and techniques referenced and described in this document should provide useful guidelines to industry and government information system professionals at large. Tailoring these products to your specific requirements and applying them to your information systems is your responsibility.

APPENDIX A

Privacy consciousness during the design phase of an information system is essential. The systems designer must be aware of the privacy implications and provide appropriate safeguards from the time the information is collected through its use and final disposition.

A generalized information system is illustrated as Exhibit A-1. This flow chart contains references to specific sections of the Privacy Criteria which is included as Appendix B. These criteria will enable the system designer and operator to better understand the privacy implications and the considerations involved in information systems.

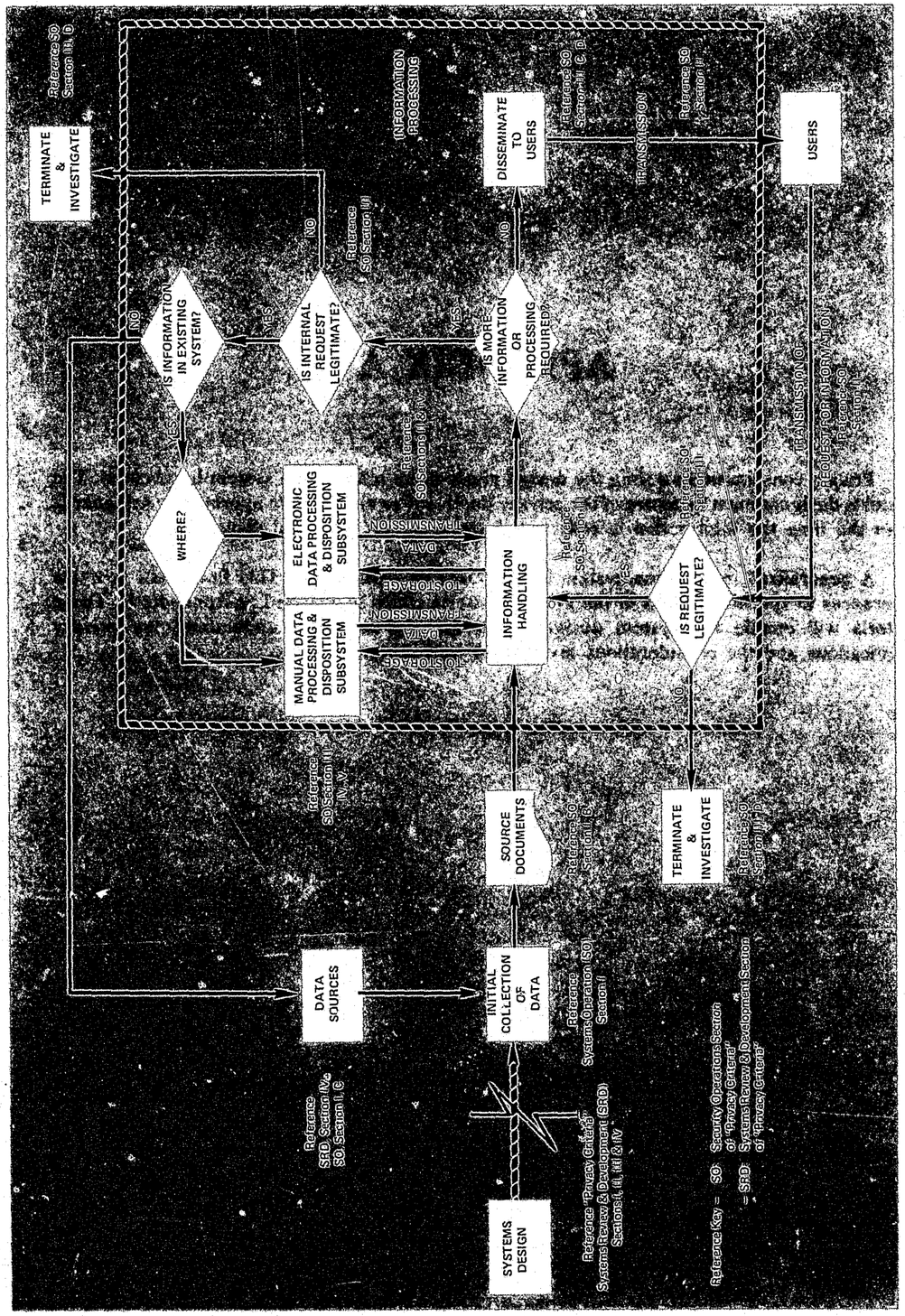


EXHIBIT A-1 PRIVACY CONSCIOUSNESS IN A GENERALIZED INFORMATION SYSTEM

APPENDIX B
CRITERIA FOR MAINTENANCE OF PRIVACY IN INFORMATION SYSTEMS

This outline provides a series of questions related to the issue of privacy in information systems. These questions will serve as a guideline for people developing, reviewing and operating personal information systems. The intent is that they be used as a device for measuring existing practices within a system against those of a model designed to maximize the privacy interest. The Guidelines are divided roughly into two parts:

- The Design or Development State of a System, and
- The Actual Systems Operation.

These guidelines are intended to be used in conjunction with the generalized information system flow chart included as a reference in Appendix A.

SYSTEMS REVIEW AND DEVELOPMENT

Users and operators of information systems are responsible for the protection of privacy within the system. This responsibility includes a concern for answers to the following questions.

- **PURPOSE OF THE SYSTEM**

A. What purposes are or will be served by the system and the information collected?
B. Can those purposes be served without collecting the information?
C. Is the information gathered worth the cost of gathering and maintaining it?

1. What commitment of economic resources is required by the system?
2. What resistance might be generated by the information-gathering process?

D. Is the information to be collected limited to the purposes for which the system was designed?

1. Is the proposed information system limited to the collection of information essential to the functioning of the program?
2. Is the information to be collected necessary only for the purpose of increasing the versatility or ease of operation of the program?
3. Is the information to be collected irrelevant to the purposes of the program?

Suggestions:

Compile an inventory of information-related forms.

Review information-related forms against these criteria.

- **SYSTEMS MANAGEMENT FOR PRIVACY**

A. Does the system provide a clear delegation of responsibility for privacy and security of information within the system?

1. Does the system provide a clear delegation of responsibility for decision-making regarding dissemination of information from the system?
2. Are the proposed or existing disseminations necessary to the purposes for which the system was created?
3. Does the system include an awareness of the existing legal protections and prohibitions against unwarranted dissemination?
4. Is the dissemination limited to institutions and/or persons who have a clear right to the information in compliance with the purposes for which the system was created?
5. Does the system include reasonable provisions for the participation of the subject in dissemination proceedings?

B. Is the system designed to minimize foreseeable privacy problems arising from non-routine requests?

1. Are decisions regarding non-routine dissemination of information limited to the persons designated responsibility for general dissemination.
2. Is non-routine dissemination limited to institutions and/or persons who have a clear right to the information in compliance with the purposes for which the system was created?
3. Does the system provide all reasonable technical and procedural protections against unwarranted dissemination?
4. Does the system include provisions for investigation of unwarranted attempts at intrusion into the system?
5. Are information-related forms designed to maximize the security of the information against unwarranted dissemination?

C. Is the system designed to minimize the collection, use and dissemination of erroneous or unreliable information?

D. Does the design of the system provide for the disposition of information with maximum deference to privacy concerns?

1. Does the disposition system include development of a complete picture of storage locations?
2. Does the disposition system include an analysis of the location of each copy of a record and the inclusion of all such locations in a disposition plan?
3. Does the disposition system include an analysis of the purposes of the information system, directed specifically at the question of disposition?

   a. Does such an analysis balance the need for future use of the information against the cost of expungement?
   b. Does the analysis include a provision for input from the subject of the record?

4. Does the disposition system include a systematic procedure for expungement of information where the analysis indicated it is a necessity?

- **EDUCATION FOR PRIVACY**

A. Does the system include procedures for educating personnel about privacy concerns and the particular policies and procedures applicable to their area of responsibility?

1. Does the education process include a provision designed to generate an understanding of the purposes for which the system was created?
2. Does the education process include a clear articulation of systems-wide policies and procedures for protection of privacy?

B. Does the system include sanctions for violation of privacy protective procedures?

C. Does the system include protection for personnel when they act in conformance with protective procedures?

- **ROLE OF THE SUBJECT IN INFORMATION SYSTEMS**

A. Does the system include reasonable provisions for the subject of a personal information system to be informed about (1) the existence of the system and (2) his rights regarding participation in the system?

Suggestions:

Provision of general public notice through publication.

Inclusion of a notice with other necessary communications with the subject.

Special notice directed specifically at informing the subject.

B. Does the system include a reasonable provision for the subject to obtain information about himself contained in the system?

C. Does the system include reasonable procedures whereby the subject may contest the accuracy or relevancy of the material about himself contained in the system?

SYSTEMS OPERATIONS

No information system, no matter how well designed, can effectively maintain privacy, unless those responsible for the routine operation of the system are committed to protection of privacy within the system. Such a responsibility includes a concern for:

- **DATA COLLECTION**

A. Is the data actually collected limited to the purposes for which the system was designed?

B. Are the procedures by which the data is collected designed to maximize the protection of such data?

1. Where possible, is data gathered in the form of anonymous statistics?
2. Where possible, is data gathered in a manner which minimizes the usage of personally identified information?

C. Is the data collected in a manner which recognizes the dignity and rights of the subject of the data?

1. Where participation in the information system is optional for the subject, is he meaningfully apprised of his rights not to participate?
2. Where information may legally be collected without the consent of the subject, is the manner of collection designed to minimize the intrusion on his privacy?

D. Is the data collected in a manner designed to exclude inaccurate or unreliable data?

- **TRANSMISSION OF INFORMATION**

A. Is the amount of movement of information reduced to the minimum necessary?

1. Is information transmitted directly to the next station essential to its function within the system?
2. Is the method of transmission one which minimizes the amount of movement of the information?

B. Is the time in which information is transmitted the minimum necessary?

1. Is information accumulated for batch transmittal as soon as it is received?
2. Is the method of transmission one which minimizes the time in which information is transmitted?

C. Does the system provide for employment of the most secure method of transmission of information?

1. Does the transmission method include segregation of sensitive or personally identifiable information from ordinary information?
2. Does the transmission method make use of physical or technical protections against unwarranted dissemination (e.g., scrambling devices, locks, seals)?

- **INFORMATION PROCESSING**

A. Is the information collected processed promptly and dispatched to permanent storage or expungement?

B. Is the exposure of information limited to the persons essential to processing?

1. Is the confidential information included in the records limited to that necessary for fulfillment of the purposes of processing, with personal identification separated from substance wherever possible?
2. Are storage security requirements detailed below applied to temporary as well as permanent storage?
3. Is the reproduction of information limited to valid processing requirements?

C. Is the routine dissemination of information from the processing stage exercised with maximum concern for privacy?

1. Who is responsible for routine dissemination of information?
2. Is capability for dissemination limited to that person?
3. Is dissemination to appropriate users processed promptly and efficiently?

D. Are non-routine disseminations of information handled with maximum concern for privacy?

1. Are there guidelines available for handling non-routine requests, and, if so, are they followed?
2. Should the inquiry be referred to another level of authority within the system?
3. Is there a provision for investigation of non-routine requests, and, if so, is it adequate?

- **MANUAL AND ELECTRONIC STORAGE**

A. Does the storage include the provision for physical security for information?

1. Does this secure storage apply to both manual and electronic storage?
2. Does this secure storage apply to records en route?
3. Does this secure storage apply at each storage location?
4. Does this secure storage include security beyond normal working hours?

B. Is there a provision for maintenance of a record of information users from storage?

C. Where the log reveals a pattern of non-routine uses of information, are there provisions for notifying the persons responsible for dissemination decisions?

- **DISPOSITION OF INFORMATION**

A. Is the retention period for information at each storage location clearly delineated?

B. Are there provisions for secure disposition of information which is no longer required?

APPENDIX C

The following two-part questionnaire will help your personnel make the necessary information privacy considerations for each program within your organization. The questionnaire is designed as a fact-finding tool for gathering data prior to the actual creation and establishment of an information privacy program. It is not intended to be all-inclusive, but should provide you with adequate information to make the basic decision, "Do we have the potential for an information privacy problem?"

The two parts of the questionnaire are broken down as follows:

- Part 1 — Manual Processing
- Part 2 — Electronic Data Processing

PRIVACY QUESTIONNAIRE

INSTRUCTIONS:

1. If the operations of your department are uniform with regard to gathering, storage and treatment of information, treat the department as one program for purposes of this questionnaire.

2. If your department includes several programs or sections which handle information in different manners, fill out a separate questionnaire for each program. (For example, if your department is responsible for administering several separate statutes, the types of information required by each program or section may vary. The manner in which information is gathered may also vary. For one program, the department may receive forms from non-employees. For another, the department may send out its own inspectors who fill out the initial report. Each of these programs should be covered by a separate questionnaire.)

3. If this questionnaire does not require all the information you can produce regarding your department's record-keeping operations, add any substantive information to the blank sheet attached.

4. All of your programs may not have privacy implications. If you decide to omit a major part of your operations, please state reasons.

5. A "record" is a collection of one or more pieces of information on a single identified individual.

Department: _____

Co-ordinator: _____

Program or Section: _____

Address: _____

Sources of information (if different from co-ordinator): _____

_____

MANUAL PROCESSING

- **INTRODUCTORY SURVEY:**

1. Describe generally the kinds of records you maintain on individuals.
2. What categories of subjects are covered?

   ☐ a. Employees.
   ☐ b. Clients receiving direct service from department.
   ☐ c. Clients receiving indirect service from department, including complainants.
   ☐ d. Clients receiving service from non-department institution.
   ☐ e. Persons not actually receiving a service from department.
   ☐ f. Institutions (as distinquished from actual humans). Specify type. Note: an institution may sometimes fit into one of the above categories.

3. How are subjects identified in your records?

   ☐ a. Name
   ☐ b. Address
   ☐ c. Social Security Number
   ☐ d. Internal Code
   ☐ e. Other

- **INFORMATION GATHERING**

1. Can you describe the specific category of individual on whom records are gathered?

2. What are the sources of your records?

   ☐ a. The subject himself applies for a state service or license.
   ☐ b. The subject himself submits a legally required report to your department.
   ☐ c. A private institution submits a legally required report to the department.
   ☐ d. A private institution voluntarily shares information with the department.
   ☐ e. Another government agency fulfills a legal obligation to share information.
   ☐ f. Another government agency voluntarily shares information with the department.
   ☐ g. The department itself generates a record through its operations.
   ☐ h. The department itself is legally empowered to conduct investigations and produce a record.
   ☐ i. The department gathers information from the public record.
   ☐ j. Complaint to department from third party.

3. Specify the sources further, if you can (e.g., which institutions submit information; what are the job titles of state-employed inspectors).

4. Are the sources of information identified on the individual records anywhere in your records, or elsewhere?

5. If so, where?

6. Who determines what kind of records are kept on individuals? Specify.

   ☐ a. The law requires certain information.
   ☐ b. Agency executives determine what information is needed.
   ☐ c. External standards (federal government, national professional organizations). Specify.

7. Specify further the sources of information policy within the department (names and levels of sources of responsible persons).

- **INFORMATION INPUT**

1. By what means do records arrive in the custody of your department?

   a. By department employee.

      ☐ (1) mailed in
      ☐ (2) telephoned in
      ☐ (3) brought in
      ☐ (4) computer terminal

   b. From outside agency.

      ☐ (1) mailed in
      ☐ (2) telephoned in
      ☐ (3) brought in
      ☐ (4) computer terminal

   ☐ c. Department creates record internally.

2. What department personnel receive the information? (list)

3. Are copies made of the records?

4. If so, to whom are those copies sent? (list)

5. Do the recipients of those copies transmit the information further? If so, to whom?

6. Are the records altered by addition or deletion of any information? If so, how?

7. Are the records stored within the department?

8. If so, in what form are they stored?

9. Who has actual physical access to stored records? This question is meant to cover both authorized and unauthorized access. Use your imagination, but obviously no one could foresee every possible access.

10. Do you know of any reason access to those records should be limited? State.

11. Is access to such records limited?

12. How is such access limited?

13. Are any other methods employed to protect the confidentiality of such records?

- **INFORMATION HANDLING**

1. Do you verify in any way the information coming in?

2. If so, how?

3. Do you update or correct the records as new information becomes available?

4. If so, how?

5. If so, how frequently?

6. Do you purge the records as information becomes dated?

7. If so, what are your standards?

8. Are correction, updating and purging applied to all sites of multiple-copy records?

9. Is the subject of the record informed that a record is being created about him or her? If so, how?

10. Is the subject's consent required when a record is created? If so, how?

11. Is the subject informed about later changes in his or her record?

12. Is the subject allowed access to or copies of his or her own records?

13. If access is allowed, under what circumstances?

14. Is a subject allowed to (a) correct, (b) update, or (c) purge information contained in his or her record?

15. If so, under what circumstances?

16. Is a subject informed about any use made of his or her record?

17. Is his or her permission required before the record may be used in any way?

18. What use does the department make of the records?

- ☐ a. General statistical analysis.
- ☐ b. Action on the individual issue.
- ☐ c. Commerical purposes (including sharing).
- ☐ d. Non-commerical sharing.
- ☐ e. None.
- ☐ f. Other.

19. Does the department keep a record of file users?

20. Are records made available to outsiders?

21. If so, to whom are the records available?

- ☐ a. To other government agencies within the state.
- ☐ b. To other government agencies generally.
- ☐ c. To commerical institutions.
- ☐ d. To private persons or institutions.

22. What is the procedure for making information available to outsiders?

23. Are there any limitations on sharing information with outsiders?

24. Are there any provisions for notice to the subject when outsiders request information?

25. Are you aware of any externally imposed restrictions on your handling of information (laws, regulations)?

26. Do you impose any voluntary restrictions on your information handling? If so, please describe.

ELECTRONIC DATA PROCESSING

This portion of the questionnaire should show the path(s) of your records until they pass out of your hands and into the Electronic Data Processing section.

1. How does your department utilize the record-handling facilities of EDP? (Describe the process by which your records reach the stage of electronic data processing.)

2. Do you transmit records to EDP?

3. In what form do you send your records to EDP?

4. Do you transmit fewer than all records to EDP?

5. Do you maintain any duplicates of records to EDP (including manual records)?

6. Where do you maintain duplicates of records sent to EDP?

7. What record handling services do you receive from EDP?

8. In what form do you receive information from EDP?

9. Who within your department has access to your record information requested from EDP?

10. Is such access limited?

11. Are any methods employed to protect the confidentiality of such information?

APPENDIX D
USING DELPHI TO ESTIMATE PERFORMANCE DEGRADATION

The Delphi Technique is a systematic estimating procedure designed by the RAND Corporation. This procedure was used during the Project to estimate the system degradation caused by the Resource Security System (RSS) in an attempt to determine Delphi's value for estimating performance of software systems in general. Software personnel from all four study sites were involved in this procedure.

Four specific indicators of performance were identified:

- CPU time billed back to the problem program (i.e. gathered by SMF).
- Number of EXCPs billed back to the problem program (i.e. gathered by SMF).
- CPU time not billed back to the problem program.
- Number of EXCPs not billed back to the problem program.

Delphi was used to estimate the percentage increase for each of these indicators after installation of RSS.

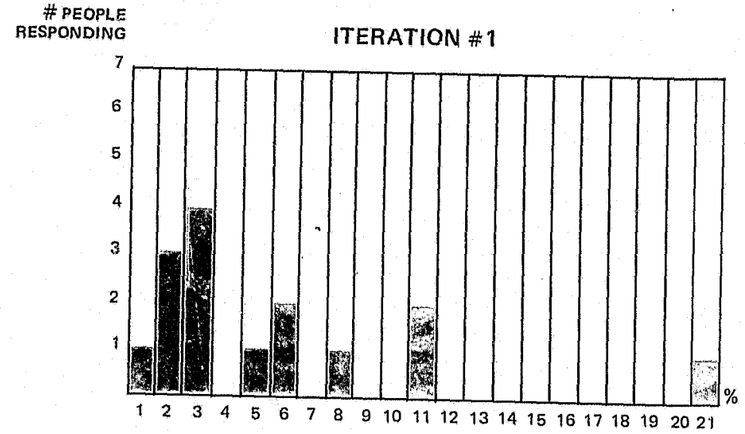
Although four iterations of the procedure are desirable, it was only possible (due to timing and communication problems between the study sites) to obtain two complete iterations. Nevertheless, the results appear to indicate that the technique is a viable estimating procedure. The results are illustrated below as histograms in Exhibits D-1, D-2, D-3, and D-4.

Each iteration is an updated estimation based on the results of the previous estimates. After each estimation, the respondents were informed of the previous response distribution in terms of its median and its interquartile range (IQR) — the interval containing the middle 50 per cent of the response.

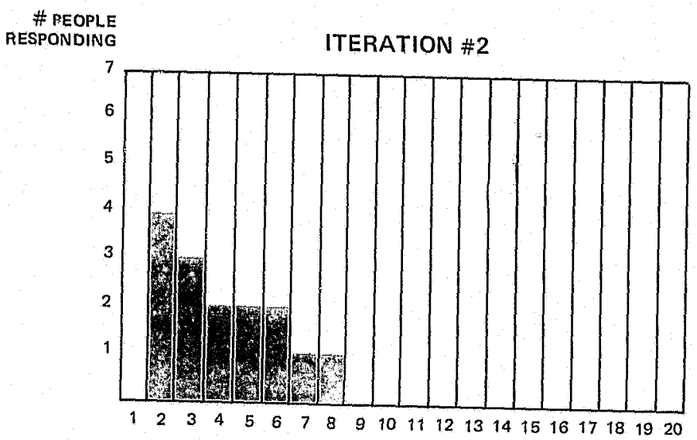
The procedure is designed to generate what may be considered an anonymous debate. Thus, in the second round, if a respondent's revised answer fell outside the interquartile range, he was asked to state briefly why he felt so strongly that the degradation would be that much less (or that much more) than the respondents within the interquartile range. Those without strong convictions tended to move their estimates closer to the median, while those who felt that they had a good argument tended to retain their original estimate and defended it.

In the third round, the respondents were given a concise summary of all reasons in support of extreme positions and were asked to base any revision of their estimates upon consideration of these reasons. Moreover, if a respondent's revised answer fell outside the new interquartile range, he was asked to state why he was not persuaded by the opposing argument. (The comments made by each of the estimators were, of themselves, a valuable source of information.)

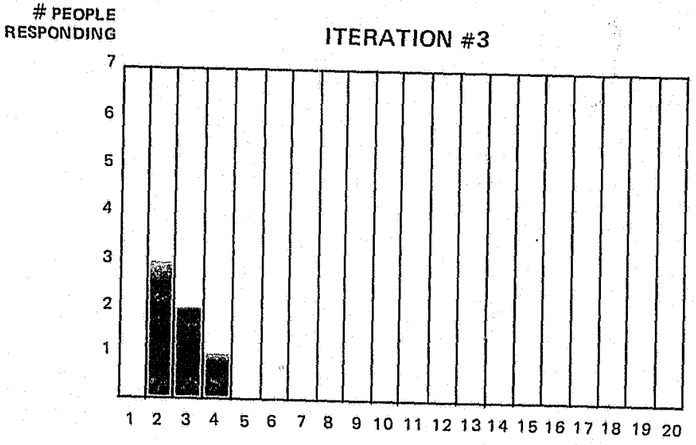
This procedure can be extremely helpful if you are entertaining the thought of installing a new software system and are interested in its impact on system performance. Since the estimators are anonymous, they are much more likely to commit themselves to an estimate because the procedure alleviates their culpability consciousness.



TOTAL PEOPLE RESPONDING = 15
MEAN = 4.8
MEDIAN = 2
MODE = 2
INTERQUARTILE RANGE: = 1% to 7%
STANDARD DEVIATION = 6.4

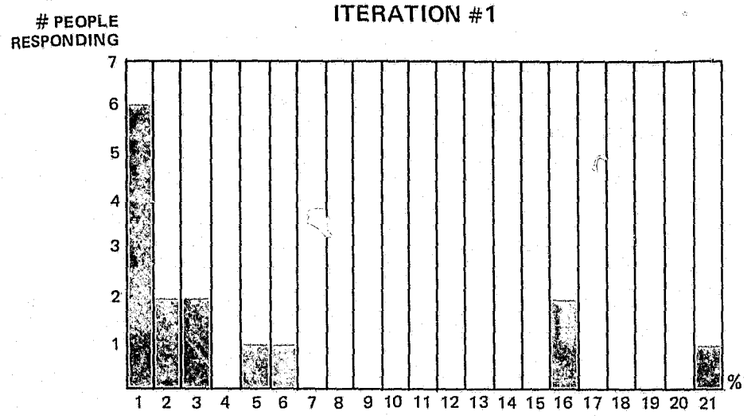


TOTAL PEOPLE RESPONDING = 15
MEAN = 3.1
MEDIAN = 3
MODE = 1
INTERQUARTILE RANGE: = 2% to 4%
STANDARD DEVIATION = 2.39

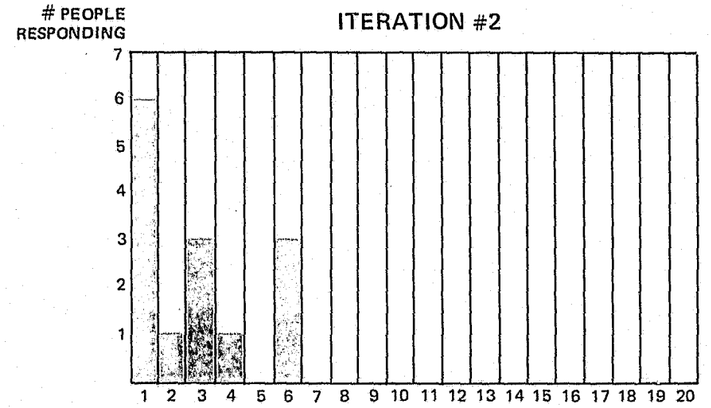


TOTAL PEOPLE RESPONDING = 6
MEAN = 1.66
MEDIAN = 1.5
MODE = 1
INTERQUARTILE RANGE: = 1% to 2%
STANDARD DEVIATION = .8

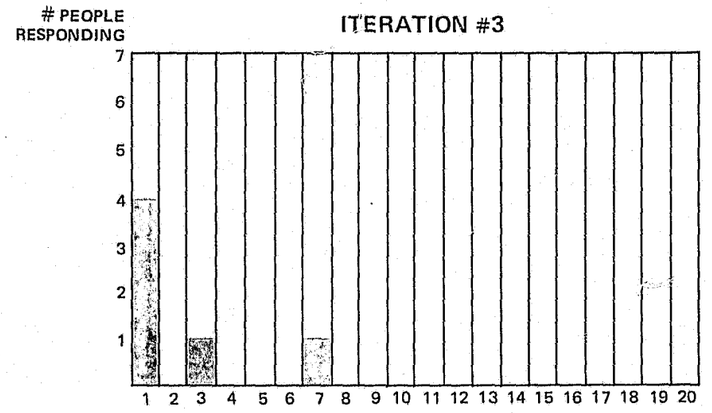
EXHIBIT D-1 DELPHI ESTIMATION FOR CPU TIME BILLED BACK TO PROBLEM PROGRAM



TOTAL PEOPLE RESPONDING = 15
MEAN = 4.33
MEDIAN = 1
MODE = 0
INTERQUARTILE RANGE: = 0% - 5%
STANDARD DEVIATION = 6.65

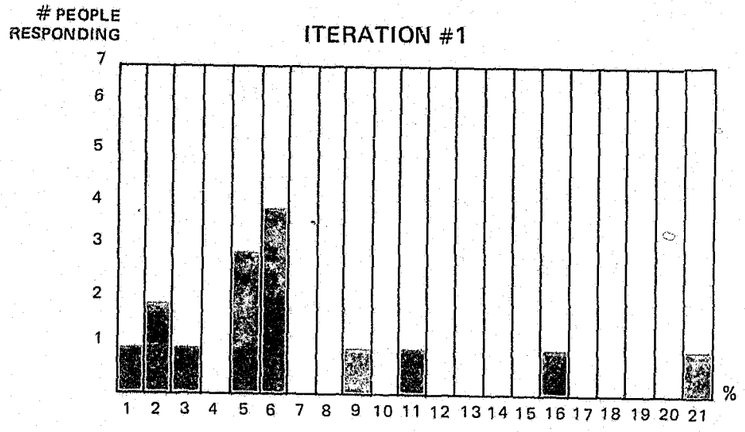


TOTAL PEOPLE RESPONDING = 15
MEAN = 1.73
MEDIAN = 1
MODE = 0
INTERQUARTILE RANGE: = 0% - 3%
STANDARD DEVIATION = 1.95

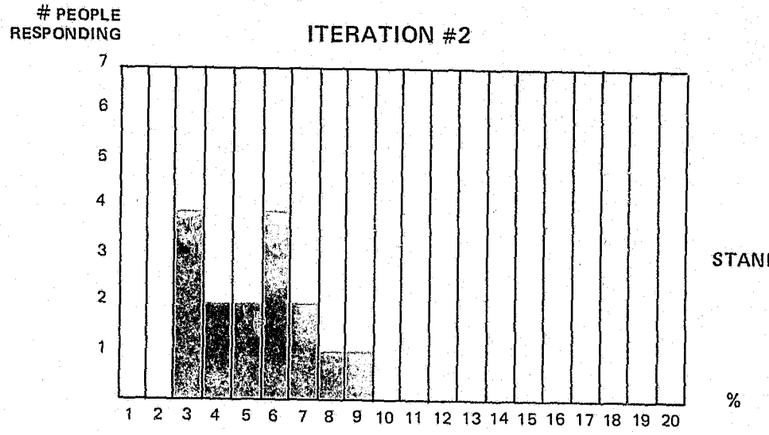


TOTAL PEOPLE RESPONDING = 6
MEAN = 1.33
MEDIAN = 0
MODE = 0
INTERQUARTILE RANGE: = 0%
STANDARD DEVIATION = 2.42

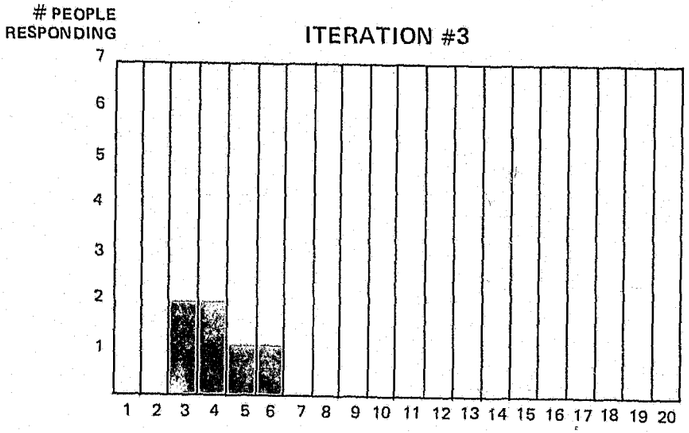
EXHIBIT D-2 DELPHI ESTIMATION FOR NUMBER OF EXCP'S BILLED BACK TO PROBLEM PROGRAM



TOTAL PEOPLE RESPONDING = 15
MEAN = 5.93
MEDIAN = 5
MODE = 5
INTERQUARTILE RANGE: = 2% to 8%
STANDARD DEVIATION = 6.66

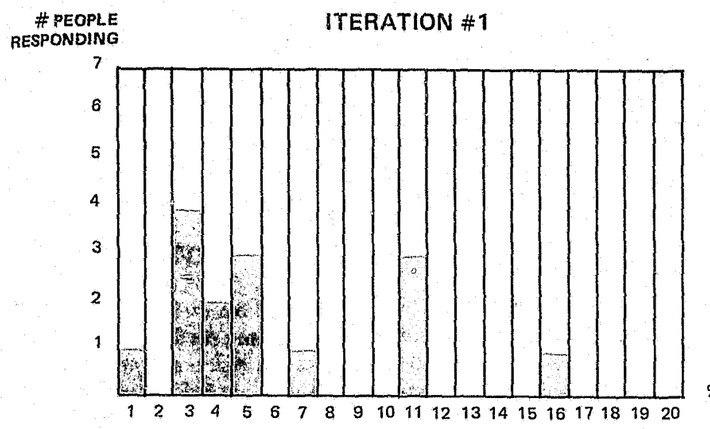


TOTAL PEOPLE RESPONDING = 15
MEAN = 4.4
MEDIAN = 5
MODE = 1.5
INTERQUARTILE RANGE: = 3% to 5%
STANDARD DEVIATION = 2.35

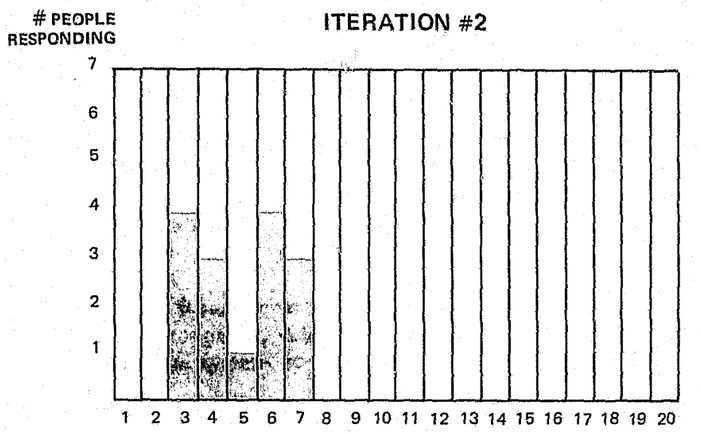


TOTAL PEOPLE RESPONDING = 6
MEAN = 3.17
MEDIAN = 3
MODE = 2.3
INTERQUARTILE RANGE: = 2% to 3%
STANDARD DEVIATION = 1.16

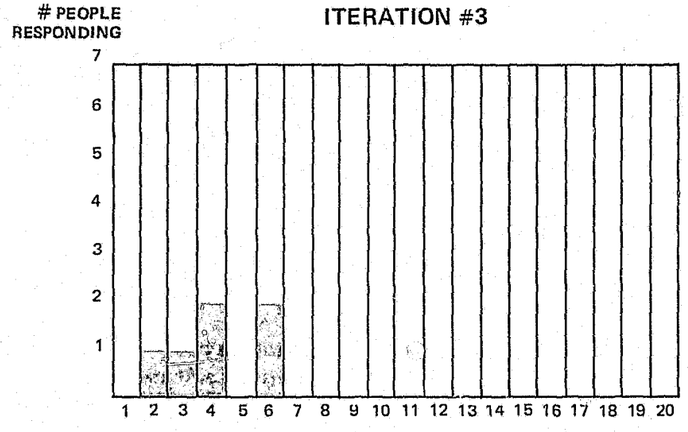
EXHIBIT D-3 DELPHI ESTIMATION FOR CPU TIME NOT BILLED BACK TO PROBLEM PROGRAM



TOTAL PEOPLE RESPONDING = 15
MEAN = 5.13
MEDIAN = 4
MODE = 2
INTERQUARTILE RANGE: = 2% - 6%
STANDARD DEVIATION = 4.23



TOTAL PEOPLE RESPONDING = 15
MEAN = 3.93
MEDIAN = 4
MODE = 2.5
INTERQUARTILE RANGE: = 3% to 5%
STANDARD DEVIATION = 1.58



TOTAL PEOPLE RESPONDING = 6
MEAN = 3.17
MEDIAN = 3
MODE = 3.5
INTERQUARTILE RANGE: = 3% to 5%
STANDARD DEVIATION = 1.61

EXHIBIT D-4 DELPHI ESTIMATION FOR NUMBER OF EXCP'S NOT BILLED BACK TO PROBLEM PROGRAM

APPENDIX E

INTRODUCTION

The Resource Security System (RSS), using OS/MVT as a base, was developed to provide protection from unauthorized reading, manipulation or destruction of user data. This protection was implemented on a test installation basis by taking advantage of the built-in security mechanisms of the 360/370 machine architecture (storage protect keys, privileged instructions, privileged operating states, etc.), through the design of virgin software routines and the modification of existing OS modules.

RSS provides five basic complementary security characteristics:

- **Integrity**
- **Identification**
- **Authorization**
- **Surveillance**
- **Isolation**

The software security performance study was executed to determine the impact of RSS on system throughput, teleprocessing response times and job turnaround, and to determine whether the system or user jobs absorb the expected degradation.

Specifically, the considerations which prompted this study are:

- What is the **total impact of degradation** on the production system at MID?
- Can a **method** be developed **to assess** the general applicability of performance results to other systems?
- Is the **cost of security** absorbed as overhead in system functions or are the user problem programs charged?
- What are the **incremental costs** associated with each security option/feature?

Due to the nature and design of RSS, it was apparent that these questions could not be answered by analyzing the production system alone. Therefore, a controlled environment study was established to address some of these considerations and to allow the Project to generalize its performance findings to other installations.

Since the results of the controlled environment analysis are more meaningful to a wider audience, this analysis is described in some depth later in this Appendix.

MEASURING THE PRODUCTION SYSTEM

- **Software/Hardware Configuration:**

The MID data center provides data processing services for thirty State of Illinois agencies. The hardware used to support this operation consists of 2 independent 3 Megabyte 370/165 central processors, 2 fixed storage units, tapes, disks (shared), unit record gear, teleprocessing controllers, and channels as configured in Exhibit E-1. Software support includes HASP/RJE, CICS, IMS and ALTER (an on-line text editing system).

Each system contains one drum on which resides the job queue, the SVC library, the HASP overlay library and a small Link library. Most of the other system libraries are maintained as one copy on shareable disk. In the case of RSS, the load library and profile data sets are maintained on a separate disk volume.

In conjunction with the performance measurement, the system configuration remained static unless a required change could not be postponed. Likewise, the operating RSS and standard OS (STD) systems were congruent in a number of respects, including:

- All data center hardware was on-line, operational and identically configured (including shareable disk),
- System disk volumes were mounted on the same channels/devices,
- DB/DC disk volumes were mounted on the same channels/devices,
- Same number of initiators were active,
- TP control regions were started in the same sequence with all of dynamic storage available,
- The operating system catalog and parameter libraries were identical,
- Residual temporary data sets were scratched each morning,
- The priorities assigned to the TP control regions remained unchanged.

- **Indicators of Degradation:**

It is possible to gather an enormous amount of data with the variety of measuring techniques and report generating programs available. The data recorded, however, served one of two purposes. Either it was a direct indicator of the degradation, or it was data concerned with identifying the type and volume of work within the production system. The latter indicator was necessary to correlate the indicators of the first type. In reviewing all possible data, the following indicators were chosen:

List 1 Direct Indicators of Degradation

- CPU Utilization — the amount of processor cycles required to process the production workload.
- EXCP Count — the number of channel programs required to process the production workload.
- TP Response Times — the elapsed time between transaction entry and system response to the terminal.

List 2 Workload Analysis (per a given time interval)

- Job Count — the number of jobs processed.
- CICS Analysis — file reads and file updates.
- Job Elapsed Time — the average time from job initiation through termination.
- ABEND'S — the number of abnormal job terminations.
- MOUNT Requests — the number of times an unloaded I/O volume is called.

- **Measurement Tools/Techniques:**

Data was collected from several sources, including:

OSPT1 — This software performance monitor measured:

- Total CPU utilization
- Total channel utilization
- Total EXCP count.

SMF — the OS System Management Facility maintains a record of many job status indicators. Included within this study were those of:

- Job count,
- ABEND's,
- MOUNT's,
- average job elapsed time,
- problem program issued EXCP's, and
- problem program CPU utilization.

CICS — CICS maintains statistics throughout its execution which relate to various resource utilizations. Analyzing a subset of this information provides some feel for the CICS workload. Included are the number of file reads and file updates. To complement this data, SMF statistics for CPU utilization and EXCP counts were gathered for CICS.

Measured Transactions — Three IMS and three CICS production TP transactions were used in gathering response time data. Transactions were entered via switched facilities during both STD and RSS production. A stopwatch measured response times.

- **Difficulties**

Several difficulties arose in measuring the production system and correlating the data. The following overview describes these factors.

- It was necessary to use on-line production data bases (IMS, CICS) for the measured transactions. This method precludes the possibility of gathering unrealistic test data base statistics. To access user agency data bases, the study was restricted to inquiry functions only.

- The Fetch Protection capability was disabled on one machine. This action was necessary because 80 to 90 production jobs were abnormally terminating due to poor coding practices such as accessing freed main storage areas. These jobs were subsequently restricted to execution on the non-Fetch Protected machine.

- The correlation of OSPT1 and SMF data is a problem due to the recording methods used. OSPT1 provides statistics from the beginning to the end of a pre-specified time interval. SMF, on the other hand, records data during job and job step initiation/termination, any of which may occur outside the measured interval. For example, a one-step job executed single thread may initiate before the measured interval and terminate following the interval. SMF would have recorded 0 EXCP executions during that time, but OSPT1 may have recorded 10,000. This problem can be reduced by selecting only those jobs which were initiated during the interval. In this way, jobs running at the beginning of the interval are recorded while jobs which remain running at the end are not recorded.

This technique tends to cause the averages of these jobs to approach the norm for the interval. Two items are of crucial importance, however, in using the technique.

The **relationship** between the length of the interval measured (I) and the average job elapsed time (E) should be such that the ratio E÷I approaches zero.

The **workload** at the beginning and end of the interval is similar.

- Reiterations of RSS installation attempts caused by software problems reduced the amount of cooperation from the MID operations staff in the data gathering phase.

- Maintaining configuration control over the complex system during the measurement period was the most difficult problem. It was necessary to divide the system into six functional areas identified as Performance Measurement Sub-systems (Exhibit E-2). Each sub-system consisted of a set of performance variables which could be categorized as controllable, uncontrollable or catastrophic; catastrophic variables are a subset of the uncontrollable variables. Exhibit E-3 summarizes these variables. All controllable variables were held constant. The occurrence of catastrophic variables caused termination of performance measurement for the affected interval. Uncontrollable variables cause effects which require smoothing to assure that RSS and STD results could be meaningfully correlated. Smoothing can be accomplished through a randomizing technique which prescribes at what times, how long and how often performance intervals are established.

As an outgrowth of this system control method, the study lived with two constraints:

Only the Local I/O, CPU, and Remote I/O sub-systems were controlled.

The randomizing technique was not developed.

The project felt that both of these problems were surmountable, but the lack of sufficient manpower prevented accomplishment.

- The length of time available in which to accomplish the production study was shortened from sixteen weeks to a five week period.

- **Assumptions**

  - The measured time interval of 7 hours was sufficiently large in order that OSPT1 and SMF data may be correlated. (E÷I = .046)
  - The system workload was approximately equal between the beginning and end of the measured time intervals.
  - The system workload was reasonably similar between the RSS and standard MVT (STD) measurement periods, and provided a representative sample of the MID job mix. (This assumption was to be analyzed during the study.)
  - A stopwatch provided sufficient accuracy to record response times.
  - The additional main storage requirements for RSS did not affect gathered statistics by a greater percentage than the percent impact on the dynamic area:

STD dynamic area	=	2568K
RSS Resident Task	=	22K
RSS Nucleus (STD)	=	10K
RSS Link Pack (STD)	=	4K
36 ÷ 2568 x 100%	=	1.4%

- The STD systems were not saturated — this situation would have affected the impact of RSS on the workload yielding inaccurate results.

- **Analysis**

In order to establish a means of relating CPU utilization and EXCP execution between systems, a measure of the respective workloads was established. This data was gathered by both software (RSS and STD) and hardware systems (A and B). The workload for each of the four systems was determined by calculating and using the toal elapsed job times per day.*

From SMF:

(Average job elapsed times)	x	(Number of jobs processed)	=	Total daily elapsed time

***Collection period — 9:30 a.m. — 4:30 p.m., weekdays.**

It was possible to determine the most important aspect of human intervention in these times by referring to the number of I/O MOUNTS requested. These requests extend the total elapsed time and were factored out to more accurately correlate the data. Requests averaged one minute to service. Thus, Total Daily Elapsed Time was reduced by: the number of requests x one minute, for each system.

ABEND's were included within the average job elapsed times and therefore require no special consideration. The ABEND data was gathered (raw data included type) so that a visual observation could determine the affect of RSS on successful job completion. This information was necessary because of the user impact involved.

From SMF and OSPT1, CPU time and EXCP statistics were correlated between the STD and RSS systems using the calculated workload levels. An analysis of the performance data gathered produced the conclusion that this particular study was not to be successful. The third assumption, that of a similar STD versus RSS workload, was violated because of two of the difficulties mentioned:

- Lack of a randomizing technique.
- Shortness of the five week study period.

The length of the study period appeared to be the most critical as it negated the possibility of including performance data from a workload which is known to fluctuate in part on a monthly basis.

The analysis showed production inconsistencies as well as direct conflicts with the results of the controlled environment measurement. As a result, no estimates of the impact on the MID production system can be provided. In light of these facts, it is important to note the last paragraph of the Conclusions.

USING THE CONTROLLED ENVIRONMENT TO PREDICT DEGRADATION

RSS can degrade a system fundamentally only by requiring longer times to execute the RSS security options. Such degradation will cause some combination of CPU supervisory, program, and wait times to increase. The following analysis determines the incremental degradation caused by each RSS option on these times as well as "overhead" added to each job by implementing RSS.

Any user can then use the degradation timings of Exhibit E-6, together with the relative speed of his machine and the characteristics of his job stream, to predict the RSS degradation to his jobs or system. Examples are given in the Conclusions.

With this thought in mind, the objectives for measuring the controlled environment were to:

- Determine who pays for security (users in increased problem program time or the data center in supervisory increases),
- Determine the incremental costs for exercising security options,
- Provide a table of degradation for general use.

Hardware/Software Configuration:

Due to the large amount of set-up and run time involved, it was impossible to schedule MID's production system for this measurement. The alternate site, Gaithersburg, Maryland, provided the following configuration during the measurement (see Exhibit E-4):

- 1 370/155-1 CPU (standard buffer support)
- 2 3330 Drives
- 4 2314 Drives
- 1 2420 Tape Unit (9/1600)
- 1 3211 Printer

Two software systems were generated immediately prior to the measurement; a STD OS/MVT 21.0 system and its counterpart RSS system. The OS JOBQUEUE, SYSIN and SYSOUT spooling functions were used. No post-generation PTF's were applied to either system. Again, as in the production setup, all operating parameters were identical.

The location of all DASD data sets/libraries appeared as follows:

- 1-2314 — Security Authorization Profile
- 1-2314 — SMF Data Sets (MANX, MANY)
- 2-2314 — Temporary data set allocation
- 1-3330 — System pack
- 1-3330 — Permanent data files

Factors of Degradation

System performance is reflected in many indicators, e.g., turn-around time, CPU utilization, etc. These indicators are influenced by degradation induced by each RSS option as well as system, hardware and job-stream characteristics. Of these influences, the RSS options can be measured on one system and used to predict the performance of any other system. These are the performance times which this controlled analysis determines. From them and knowledge of one's system, one determines RSS effects on that system. Degradation occurrs wherever RSS receives control through the operating system as well as in "overhead" due to modifications to STD system modules. The specific items which were measured were:

- Fetch Protection
- OPEN Authorization
- Surveillance Loggings
- Program Execution/Modification
- DASD Space Allocation
- DASD Sanitization
- Main Memory Sanitization
- SVC Authorization
- Direct Device Allocate/Deallocate/Buffer Sanitization
- Overhead

RSS Configurations

RSS provides the capability to select from among fourteen options those security features which are desirable at a particular site. This flexibility was provided to allow installations with diverse data security requirements to tailor the system to their needs.

Since there are fourteen options comprising RSS, there are thousands of combinations of security functions which can be used. It was, therefore, practically impossible to measure the degradation directly of all possible RSS optional configurations. Instead, three distinct RSS configurations were used to determine the degradation caused by the specific options. This technique will predict any RSS configuration degradation as well.

The **minimum configuration** (MIN) represented a system with few of the security options included. This system contained four of the five basic security characteristics. Surveillance activities were excluded.

MINIMUM CONFIGURATION

Option No.	Description of Option
1	Fetch protection is installed on the CPU.
9	All direct access space allotment authorization will be **bypassed.**
10	All program authorization will be **bypassed.**
12	Undefined users to be accepted.

The **MID** production configuration (MID) contained the option settings selected to run within the production environment. This configuration was representative of a moderately heavy usage of available features.

MID PRODUCTION CONFIGURATION

Option No.	Description of Option
1	Fetch protection is installed on the CPU.
6	Each modification of any program defined in a controlled library will be logged in the security audit trail (SMF log).
8	Each modification of a system library beginning with "SYS1." will be logged in the security audit trail (SMF log).
9	Direct Space Allotment Authorization will be **bypassed**.
12	Undefined users to be accepted.
13	All data sets will be sanitized (overwritten with zeros) when scratched if it is a level 6 or above.

The **maximum configuration** (MAX) can be considered as the RSS system providing the greatest possible protection. It was expected that this system would yield the most degradation.

MAXIMUM CONFIGURATION

Option No.	Description of Option
1	Fetch protection is installed on the CPU.
3	Each OPEN of a permanent data set will be logged in the security audit trail.
4	Each OPEN of a temporary data set will be logged in the security audit trail.
6	Each modification of any program defined in a controlled library will be logged in the security audit trail.
7	Each execution of any program defined in a controlled library will be logged in the security audit trail.
8	Each modification of a system library beginning with "SYS1." will be logged in the security audit trail.
12	Undefined users to be accepted.
13	All data sets will be sanitized when scratched if level 6 or above.

Controlled Job Stream Characteristics

A stream of sixty-three jobs programmed specifically for this analysis were to be measured within the controlled environment. The executing programs were coded so that all system resource requests were known. In some cases, the Job Control Language was coded to cause specific system requests. Knowing exactly what functions were to be executed by a single job provided the capability to associate increased resource utilization times to those functions.

The controlled job stream included:

- 3 jobs issuing only controlled SVC's.*
- 3 jobs executing only fetch instruction loops.
- 2 jobs requesting DASD space allotment.
- 1 job requesting a tape sanitization.
- 2 jobs directly allocating a hardware device (printer).
- 2 jobs executing a controlled library program.*
- 2 jobs updating a controlled library program.*
- 2 jobs updating a system library program.* (SYS1. library)
- 3 jobs GET/FREEing main storage.
- 6 jobs sanitizing DASD space.
- 1 **Baseline** job issuing no resource requests (no options executed).
- 36 jobs OPENing data sets organized by various access techniques (QSAM, QISAM, BISAM, BSAM, BPAM, BDAM) in different modes (O, IO, I, U).

Exhibit E-5 is a table which shows the expected effect of the three RSS configurations on job elapsed times. The elapsed time for the MIN runs are expected to all be higher than the STD system because of RSS overhead not tied to specific options. This overhead is a result of additional processing added to standard OS modules. The differences between elapsed times in this exhibit are a direct result of the option settings within the configurations.

The entire jobstream was designed so that any permanent data set which was allocated during the run was also deallocated. This procedure allowed jobstream re-runs without any special permanent data set considerations. In addition, job and job step parameters were held constant for all runs. In particular, the parameter TYPRUN = HOLD was used for each job to prevent automatic release from the job queue.

Performance Measurement Tools

Three measurement tools were used within the controlled environment.

- SMF was used to determine the total number of EXCP's issued and charged to the user. A comparison was made between STD and MID only.
- The Second Level SVC Interrupt Handler was modified temporarily to count the number of Type 2, 3, and 4 SVC's issued in non-zero problem state individually by job on the STD system. This data was used as input to a regression model and dictated the number of times SVC authorization routines were executed for each job. This SVC Counter was executed separately from the performance runs to avoid influences on the data.

***Requires program authorization [Option 10].**

- The Systems Measurement Instrument (SMI) is a hardware monitor physically connected to the system hardware. The SMI was used to record by job:

  1) WAIT State
  2) Key 0 Processing*
  3) Non-Key 0 Processing (Problem Program)
  4) Device busy time for the SMF volume
  5) Number of SEEKS to the profile data set.

  The data from items 1, 2, 3, and 4 were used as the input to the regression model. Item 5 was reviewed to understand the amount of profile I/O activity which was necessary to perform authorization functions. In the event of significant degradation, item 5 would prove useful as an isolation factor.

The Measurement Technique

The measurement technique used within this environment involved several considerations prior to the execution of the measurement itself:

- The physical location of two DASD data sets; the profile data set and the SMF data sets. In order to determine the degree of degradation incurred by authorization profile accesses, it was necessary to build and isolate the profile data set on one volume. This volume was probed using the SMI. The SMF recording data sets were isolated on another volume. This action was necessary to determine during which specific job executions SMF recording took place. The knowledge of this information allowed the factoring out of that system function from the total system times recorded for job execution. This resulted in a more accurate picture of the CPU resource required solely for job handling. This volume was also probed.

- In conjunction with the SMF data set placement, the in-core SMF buffer size was generated to its maximum allowable size (one physical DASD track) thus minimizing recording events.

- The creation of several data sets under the various data organization methods was necessary. These data sets remained unaltered throughout all jobstream executions because they were accessed by "Read Only" programs.

- It was necessary to attach the SMI to the system hardware, program the SMI logic panel, and execute test procedures to verify the validity of the SMI output. It should be noted that the logic panel was designed so that CPU "WAIT" time was recorded during the time the job was released from the queue through job termination. CPU "WAIT" before and after those processing points was eliminated.

***Referred to in Model as Supervisor State [SUPV]. Includes both Supervisor and Key 0 Problem Program States.**

The measuring technique itself may be described in a step-by-step procedure which was reiterated for each execution of the jobstream under all systems.

STEPS:
1. IPL system
2. VARY required devices on-line
3. Execute program to scratch all residual temporary data sets
4. Set options to establish MIN, MID or MAX (RSS only)
5. Read entire jobstream into jobqueue
6. Start one initiator
7. Clear SMI registers
8. Start SMI monitoring
9. Release a job
10. When job terminates, STORE SMI registers to tape
11. Repeat steps 7-10 until jobstream is terminated
12. Dump SMI data from recording tape to master tape
13. Dump SMF files to master tape
14. Start OS Writer and print job outputs
15. Stop writer
16. Repeat steps 3-15 for all subsequent runs (start at STEP 1 when switching from STD to RSS)

At the conclusion of all runs, two master tapes contained the total SMI and SMF data. The SMI data was used as the input to the regression model for analysis.

The following list provides a breakdown of the number of runs made:

- STD — 3
- MIN — 2
- MID — 2
- MAX — 1

The runs were approximately 2½ — 3 hours in length.

Data Collection Difficulties

- Two unresolved problems which occurred during the measurement eliminated some valuable output. One problem was an RSS bug which forced many jobs into abnormal termination when the space allotment authorization feature was activated. This feature was therefore eliminated from the measurement. Another problem was not evident until analysis of the model showed some inconsistent results within the DASD sanitization jobs. Even though the jobs terminated normally, a software bug caused a bypass of the sanitization operation. This measurement was therefore not recorded.

- Only one MAX run was executed. The situation however was not as detrimental as it might have been. This was the case becasue the MAX runs were to be used in measuring space authorization and DASD sanitization, both of which were inoperative. Only two logging functions remained to be measured with MAX.

- The technique used for measurement did not include reader/interpreter time. There was some RSS induced overhead in this function because OS contains an exit to identify the user name/codeword on the jobcard. This was not considered to be important since it is a single, non-complex event for each job and users are not charged for the function because it is a system task.

- Somewhat of a correlative restriction was the fact that problem program CPU time as measured and entered into the model did not agree perfectly with SMF times. SMF data was not used because of its inaccuracies.

The Regression Model

- Description:
  For the jobs in each controlled configuration, several measurements of program, supervisor, and wait times were made in order to assess the degradation caused by the options exercised by the job. A methodology was devised to separate the degradation effects caused by overhead and the use of specific options.

  The method appropriate for the required separation of effects is dictated by what is known about degradation. Namely, the difference between standard- and RSS-computing time is the sum of RSS overhead plus the degradation-time for the execution of each option the job uses, multiplied by the number of times the option is used.

  This is made explicit in the following regression model.

$$\text{Additional Time} = W + Y*N1 + \sum_{J=1}^{18} [A(J) + \{A1(J)\} * \{N2(J)\}] + B*N3 + N4*(C + D) + E*N5 + G*N6 + \sum_{K=0}^{1} N7(K)*[H(K) + X(K)* \{N8*R + N9*T\}] + L*N10 + M*N11 + P*N12 + S*Q$$

Where the coefficients to be determined by least squares analysis are:

W = Job overhead (inherent within RSS).

Y = Step overhead (inherent within RSS).

A(J) = Time to authorize the initial opening of a file by Method J. (Method J being comprised of Access Method, type of OPEN and permanent or temporary file).

A1(J) = Time to authorize all subsequent openings for the same file.

A2(J) = Time to log the event.

B = Time to authorize and log a controlled library modification (CLPMOD) (= B or 0 according to the option setting).

C = Time to log a CLP execution (CLPEXEC) (= C or 0 according to the option setting).

D = Time to authorize a CLPEXEC (= D or 0).

E = Time to authorize and log a system library modification (SLPMOD) (= E or 0).

G = Time to authorize allocation of extra DASD space (= G or ∅).

H(K) = Time to handle a sanitization request for a primary data file (excludes time to overwrite with zeroes) (= H or 0).

R = Time to overwrite a unit of disk. (sanitization) (= R or 0).

T = Average time to locate disk extent. (sanitization) (= T or 0).

L = Time to allocate/deallocate and buffer sanitize a directly allocated device (= L or 0).

M = Time for SVC authorization (= M or 0).

P = Time to overwrite a 2K block of main storage (=P or ∅).

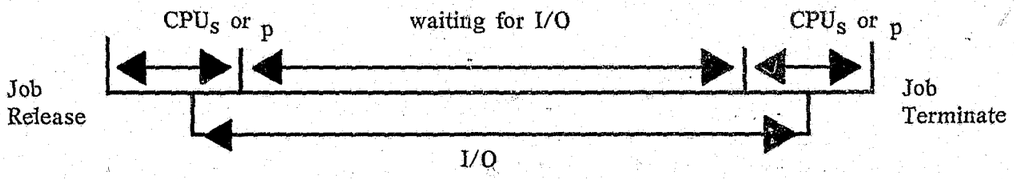
S = Fetch protect degradation as a proportional of STD run time.

Q = Total CPU time before RSS.

The variables (input parameters) for this analysis and all subsequent predictive analyses are:

N1 = The number of steps within the job.
N2(J) = The number of files OPENed by Method J.
N3 = Number of controlled library programs modified.
N4 = Number of controlled library programs executed.
N5 = Number of system library programs modified.
N6 = Number of times additional space is requested on disk.
N7(0) = Number of times to purge tape.
N7(1) = Number of times to purge disk.
N8 = Number of tracks of disk.
N9 = Number of disk extents to purge.
N10 = Number of directly allocated devices.
N11 = Number of SVC issuances.
N12 = Sum of storage requested in all the GET/FREE main's.
X(K) = 0 for tape (K=0);
= 1 for disk (K=1).

To determine the total increase in job elapsed time within the controlled single-thread environment, the CPU states were used as a reference. That is, elapsed time was considered as a summation of CPU problem program time, CPU supervisor time and CPU idle time occuring from the point of queue release to job termination, thus requiring the model to be run 3 times for the jobstream in each configuration. (Key 0 problem state is included with the supervisor times.)



- Rationale

The purpose of this analysis is to evaluate all coefficients of the model (W, Y, ...Q) using the controlled jobstream data. The least squares criterion is used to find the best fitting parameter values. (See Scheffe, *Analysis of Variance,* Wiley, 1959). Least squares gives an evaluation which is unbiased and has relatively small variability. The results of this analysis are located in the following section.

- Assumptions

This model incorporates explicitly the following assumptions, which are implicit in the previous sections:

1) RSS degradations occur only through overhead and through execution of the options.
2) Degradation due to a given option is proportional to the number of times the option is executed.

Data

- Compilation

The data represented within this section was compiled through a series of steps. These steps may be cited as follows:

Step 1: Gathering the data using the SMI.
Step 2: Data reduction consisting of two aspects:

a) Subtracting average SUPV and WAIT SMF times from jobs executing concurrently with SMF buffer dumping to DASD.
b) Transcribing the data into machine readable language to be input to the programmed regression model.

(Both functions were performed through a specially designed reduction program to speed processing and eliminate human error.)

Step 3: Processing the data with the model for supervisor, program and wait times.
Step 4: Formatting the output report.
All data is reported in milliseconds within Exhibit E—6.

- Notes regarding Exhibit E—6

1. The WAIT time to overwrite one DASD track was an estimate obtained from the IBM Storage Systems Center. This time includes approximately thirty-eight milliseconds and is provided since DASD sanitization could cause severe degradation, especially when one considers temporary data sets containing confidential information.*
2. The OPEN logging figures were all very similar and the average is provided as one figure within the table.
3. As noted previously, extra space allocation and I/O sanitization figures were not gathered.

- Notes regarding data

1. The model showed that of the 18 types of OPEN's monitored, there appeared to be 3 categories of degradation. In this light, the data was averaged by category and appears as 3 A(J)'s. This method allows for easier interpretation of the data.

A(1) — All permanent data set OPENs except ISAM
A(2) — Permanent ISAM data set OPENs
A(3) — SAM Temporary data set OPENs

2. The output from the WAIT model produced data fluctuating slightly above **and** below zero additional time. The affect that RSS had on WAIT time was therefore negligible except for the following exceptions which were not calculated into the Mean and Standard Deviation.

BSAM I/O — 10% increase in WAIT time
QSAM I — 14% decrease in WAIT time
QISAM U — 21% increase in WAIT time
QISAM I — 32% increase in WAIT time

***Note that concurrent I/O on a volume being sanitized could drive this figure upward into the sixty millisecond range.**

3. In order to obtain an indication of the repeatability of the data gathered in general, and hence its degree of accurancy, problem program (PP) time was analyzed. The SMI PP times for "like" runs was averaged and the variation calculated.

3 STD Runs — average PP time = 502,590 MS
Variation from average = +.05%, −.06%
2 MIN Runs — average PP time = 543,120 MS
Variation from average = ±.05%
2 MID Runs — average PP time = 548,276 MS
Variation from average = ±.37%

CONCLUSION

General Applicability

The data presented in the appendix can be used to predict the impact of such a system as RSS within any environment. The need to do so may be twofold. A data center may be requested to provide increased job cost information to its users. In conjunction, accounting routines may require modification. Secondly, an installation might wish to know what the total impact upon a particular system might be.

Exhibit E—6 can be used to predict the impact of software security degradation to a job or system whose characteristics are known and whose speed relative to the 370/155 are known. To predict these times, one need enter into the model the known coefficients W thru Q as given in the table and the number N1 thru N12. (These numbers must be determined through job analysis.) Predicted degradation is the resulting additional time divided by the machine speed relative to the 155.

Example 1 (Degradation to a single job)

Consider a two step job which OPEN's 3 files of Type 1, 5 files of type 3, executes a CLP and issues 100 SVC's in the process. If the CPU is 10% faster than the 370/155 and if all the appropriate options are set excluding logging, then the degradation to this job in milliseconds is:

[10.83+2(4.19)+3(33.62)+5(25.69)+8.07+100(.25)] /1.1=256Ms.
(Note that only program times are used.)

Example 2 (Degradation to a multi-programmed system)

This situation is handled in the same manner as example one with two considerations:

- Two models will be used and summed; one for program time and one for supervisor time.*
- The N's must be gathered beforehand with a software monitor routine over selected time intervals.

***WAIT time has minimum impact as previously noted and need not be considered.**

Consider the same system for which during the average hour the following functions are executed and the total CPU utilization rate is 60%:

Time Coefficents	Number of Executions(N)
W	30
Y	90
A(1)	65
A1(1)	5
A(2)	20
A(3)	100
B	10
D	60
E	10
M	15,000
P	600

Then:

Time Coefficients SUPV	PROG	x	#Executions (N)	= SUPV Tm	+ Program Tm
304.25	10.83		30	9,127.50	324.90
384.14	4.19		90	34,572.60	377.10
301.32	33.62		65	19,585.80	2,185.30
16.91	1.69		50	845.50	84.50
309.04	25.27		20	6,180.80	505.40
836.57	25.69		100	83,657.00	2,569.00
28.68	3.48		10	286.80	34.80
49.22	8.07		60	2,953.20	484.20
12.56	1.21		10	125.60	12.10
4.01	.25		15,000	60,150.00	3,750.00
5.84	.00		600	3,504.00	00.00
TOTAL:				220,989	10,327

Total Increase in CPU time = SUPV+PROG=231,316 Millisecs/hr.
Increase as an hourly percentage = 231 secs÷3600 secs x 100% = 6%

This 6% figure states that; given a set of RSS options to be executed and the knowledge of the number of times these executions will occur, the total CPU utilization will increase from 60% to 66%.

Concluding Remarks

It is interesting to observe that programming efficiency has played a role with the RSS system. RSS used in-core buffers to store authorization records from the DASD profile which it interrogated before requesting I/O. The SMI measurement showed the effectiveness of this technique by the difference in overhead between the first and subsequent OPEN's of a file. The first OPEN caused the authorization record to be brought into main storage and it was subsequently used from that location. Profile SEEKs were minimized throughout processing.

Secondly, a review of SMF output from the controlled run revealed that RSS was issuing fewer EXCP's in several of the ISAM jobs while all other jobs remained constant.

A review of BPAM OUTPUT revealed that it's efficiency had been improved significantly.

These last two items indicated that coding improvements were made to the STD system when authorization and integrity modification were inserted into existing OS modules.

Finally, the true test of the performance of any production system is reflected by the demands of the users. In the case of RSS, functional problems occurred, but no users complained of increased response time, CPU processing time, or turnaround time, and the data center recognized no decreased throughput conditions. This condition substantiates the finding of both the controlled environment study and the results of the DELPHI Technique (Appendix D).

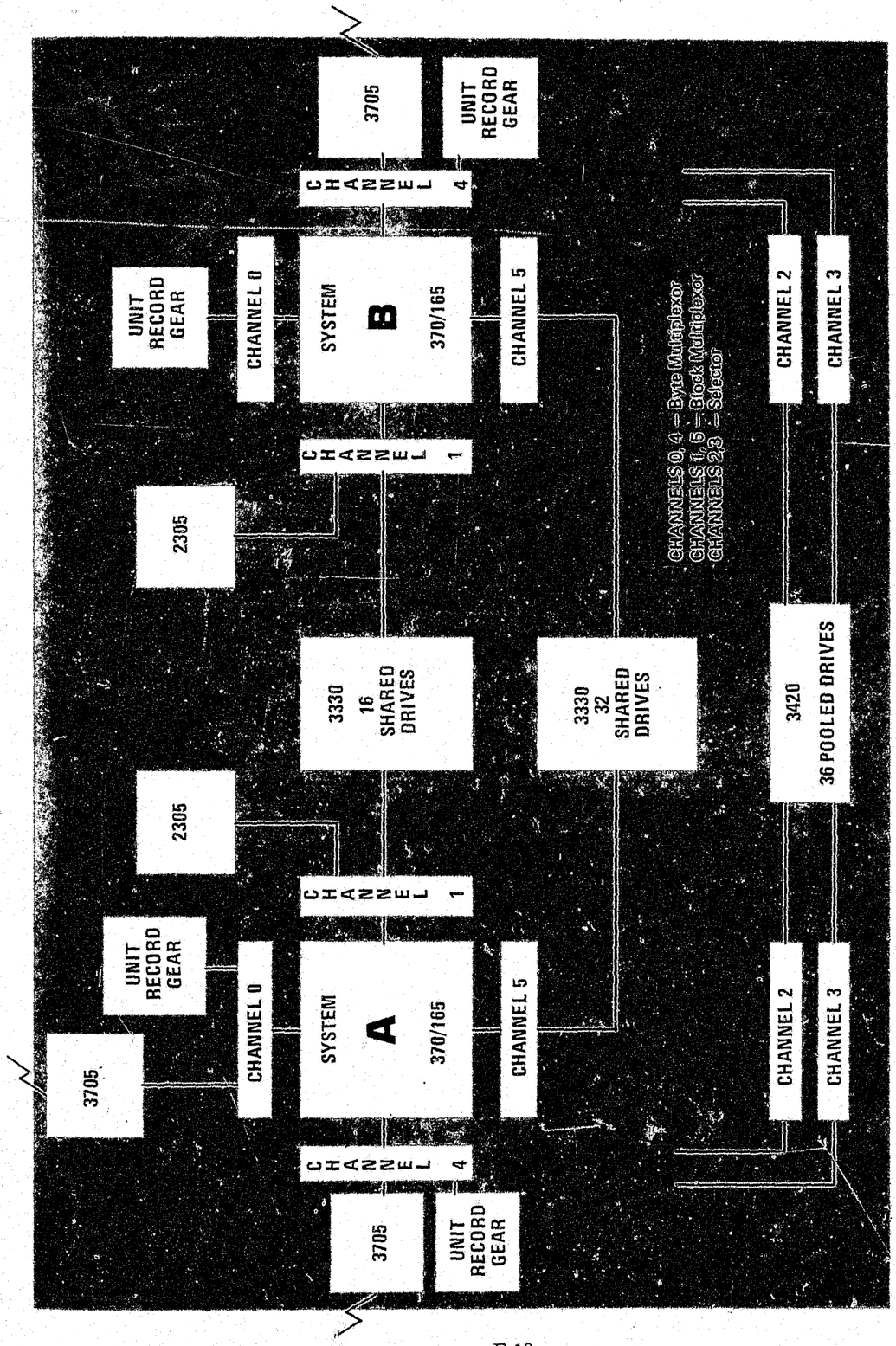


EXHIBIT E-1 HARDWARE CONFIGURATION OF MID DATA CENTER

EXHIBIT E-2 PERFORMANCE MEASUREMENT SUB-SYSTEMS

SUB-SYSTEM	INDICATORS	VARIABLES: CONTROLLABLE	VARIABLES: UNCONTROLLABLE	VARIABLES: CATASTROPHIC
1. Remote I/O	• Channel Utilization	○ # Terminals/Line ○ Terminal Types ○ # Lines ○ Line Types ○ # Transmission Control Units	• Terminal Down • Line or Modem Down • Line Quality	○ Channel Down ○ Transmission Control Unit Down
2. Remote Req.	• Response Time • # Transactions/ Time Unit • Time Last Request Processed		• Monthly Fluctuations • Weekly Fluctuations • Daily Fluctuations • Hourly Fluctuations • Programmer Attendance • Software Status	○ Agency Conditions
3. Operations Support			• Request Time Delay • # Operator Errors • # Operators	○ Operator Error
4. CPU	• CPU Utilization • Avg. Time Transactions In Queue • Avg. # Transactions In Queue	○ SYSGEN Options ○ PARMLIB Options ○ # Initiators ○ Same Sub-System Tasks ○ Same Core Allocation Same Core Allocation	• Operator Actions	○ CPU Down
5. Local I/O	• EXCP Count • Channel Utilization	○ Hardware Configuration ○ Volume Configuration ○ Library Placement	• Devices Unavailable • Sharing Devices • Error Recovery	○ Hardware Failure
6. Job Submittal (Batch/RJE)	• Turnaround Time • Thruput • Backlog Size • Job Queue Averages		• Monthly Fluctuations • Weekly Fluctuations • Daily Fluctuations • Hourly Fluctuations • Programmer Attendance • Software Status	○ Agency Conditions

EXHIBIT E-3 SUB-SYSTEM VARIABLES & INDICATORS OF DEGRADATION

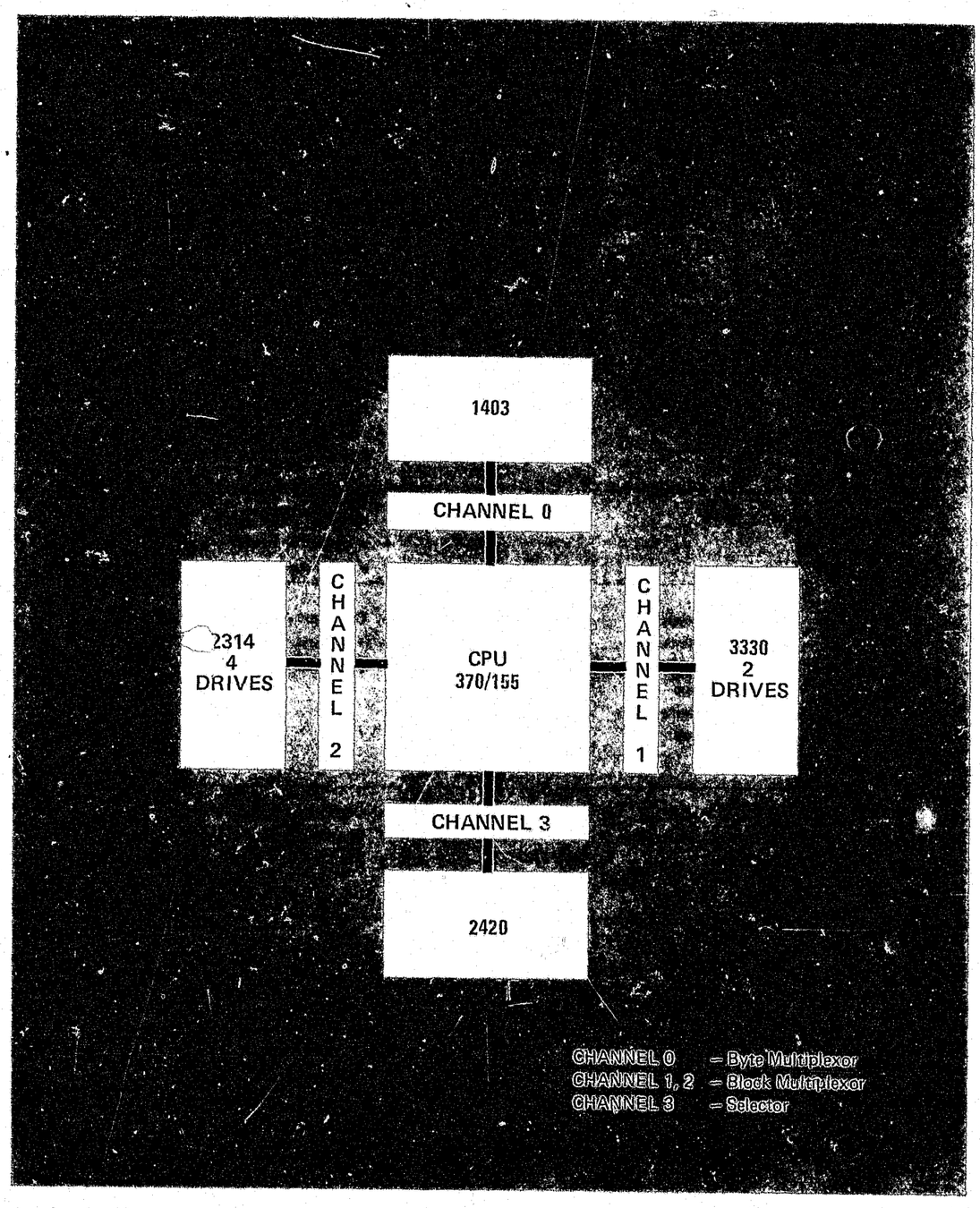


EXHIBIT E-4 HARDWARE CONFIGURATION IN CONTROLLED ENVIRONMENT

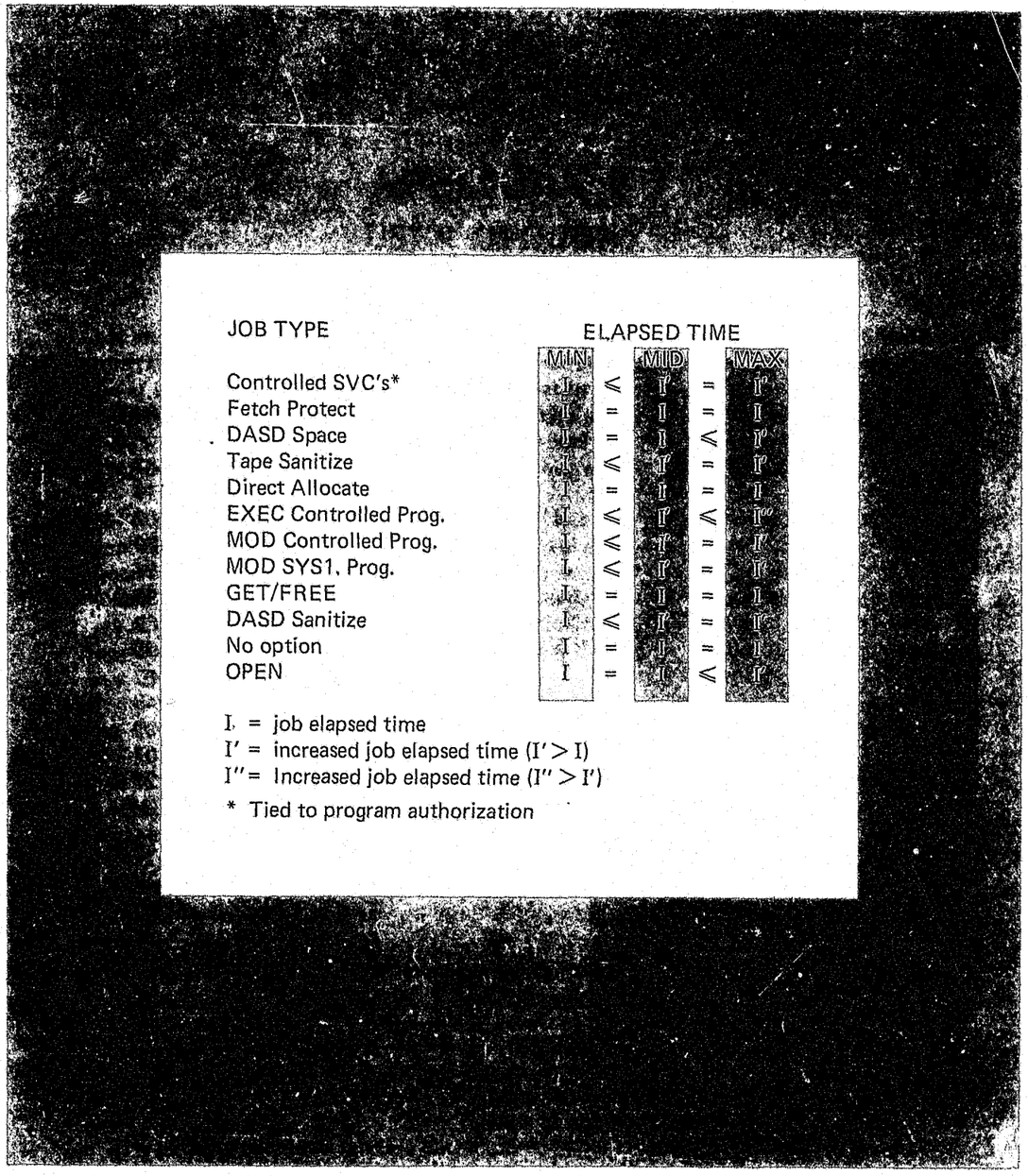


EXHIBIT E-5 RELATIVE JOB ELAPSED TIMES UNDER VARYING SOFTWARE SECURITY SYSTEM CONFIGURATIONS

TABLE OF DEGRADATIONS
(MILLISECS)

FUNCTION/OPTION	TIME PARAMETERS	SUPER-VISOR	PROGRAM	WAIT*
JOB OVERHEAD	W	304.25	10.83	
STEP OVERHEAD	Y	384.14	4.19	
1ST OPEN (TYPE 1)	A (1)	301.32	33.62	
SUBSEQUENT OPENS	A1 (1)	16.91	1.69	
1ST OPEN (TYPE 2)	A (2)	309.04	25.27	
SUBSEQUENT OPENS	A1 (2)	106.98	.95	
1ST OPEN (TYPE 3)	A (3)	836.57	25.69	
SUBSEQUENT OPENS	A1 (3)	9.56	3.30	
AVG OPEN, LOGGING	A2 (J)	8.61	1.52	
CLPMOD AUTH & LOG	B	28.68	3.48	
CLPEXEC LOG	C	24.51	52.03	
CLPEXEC AUTH	D	49.22	8.07	
SLPMOD AUTH & LOG	E	12.56	1.21	
ALLOCATE EXTRA SPACE	G	—	—	—
SANITIZATION REQUEST	H	—	—	—
OVERWRITE 1 TRACK	R	—	—	
LOCATE DASD D.S. EXTENT	T	—	—	—
DIRECT ALLOCATE AUTH	L	251.95	62.30	
SVC AUTH	M	4.01	.25	
FREEMAIN SANITIZATION	P	5.84	.00	
FETCH PROTECTION	S*100%	.00%	.00%	

* For each job, the ratio of WAIT "after" to WAIT "before" was calculated following the run of the model. These ratios were uniformly close to "1" except for those jobs requiring manual intervention, e.g. tape mount requests. This WAIT data is reported only as a Mean of 1.002 and a Standard Deviation of .050.

EXHIBIT E-6 ■ THE CALCULATED COEFFICIENTS OF THE REGRESSION MODEL

APPENDIX F
USER OPINIONS

As is often the case with projects of this magnitude and scope, reaction to Project SAFE's endeavors ranged from something short of a standing ovation applauding the state for attacking the issue of information privacy to accusations of overdramatizing an already overemphasized issue. Fortunately, most of the individuals in the state's data processing ranks appear to be concerned with the problem of information privacy and security. Unfortunately, many data processing managers are unsure of the most effective way to deal with the problem.

For the purpose of brevity, it is necessary to highlight the findings of our interactions with user agency personnel by describing briefly the results of a questionnaire that was distributed to data processing managers within the agencies subject to the Governor. The twenty-eight respondents (to the forty-two questionnaires distributed) are a fairly representative sample of the types of user's requiring MID's services. These findings are not intended to be conclusive; however, they appear to be indicative and consistent with our informal day-to-day experiences with user agency personnel.

First, on the subject of accidental or intentional disclosure of information:

- 40% of the data processing manager sample group felt that computers in their departments increased the likelihood of disclosure of confidential information over manual systems.
- 43% believed that more safeguards could be used in the design and implementation of an application system.
- Only 11% felt that they did not have adequate technical precautions (viz., software and hardware security, automated access control system, etc.) This fact confirmed our initial suspicion that very few managers are aware of the absence of protection of existing technical safeguards at MID. The subject of software operating system vulnerabilities in particular has not been, until very recently, emphasized by software manufacturers.
- 21% of the respondents felt that they required better procedural protection (e.g., sign-in procedures, disposal controls, backup procedures, etc.).
- 21% felt that they had less than adequate personnel practices (viz., screening, job rotation, education, etc.).

On the subject of the accidental or intentional destruction or modification of data:

- 36% felt that the computer increases the likelihood of the destruction or modification of data over manual systems.
- 34% felt that more attention must be given to this threat in the design of their information systems.
- 14% believed that their systems were not adequately protected by technical safeguards.
- 26% felt that their existing procedures are inadequate.
- 12% felt that their existing personnel practices need improvement.

In general:

- Most (75-85%) of the data processing managers did not consider existing data security mechanisms (viz., without a software security system) to be impediments to the efficiency of their operations.
- 84% of the respondents believed there was a need for a single decision making individual or group responsible for all data security within their organization.
- 42% of the respondents felt that existing information privacy and security education within the state is less than adequate.
- All the respondents felt that security is a responsibility that must be shared by themselves and MID. MID should be responsible for developing guidelines and standards.

Most data processing personnel will admit (with varying levels of concern) that information privacy and data security is a problem. Few, however, appear to have structured a concise analysis of the problem and fewer still appear to have developed an unemotional, well-balanced approach to its resolution. This situation certainly does not reflect on the capability of these managers to deal with the problem. Rather it reflects an inadequate understanding of the complexity and diversity of the potential threats confronting the organization and also the absence of a viable approach to creating a well-balanced security environment.

APPENDIX G

The following cases were documented during the field work to determine the ease of use of the valuation methodology. Members of the IBM/Illinois Project SAFE team met with administrators in the Office of Vital Records to assess the Birth Records System Value and in the Department of Public Health to assess the Veneral Disease Information System through the use of the valuation methodology.

The quotations used in Case 1 and Case 2 emphasize the administrators' general responses to questions and should not be interpreted as verbatim quotations of individual interviewees.

CASE 1

Office of Vital Records — Birth Records System

There are 139 birth registrars in Illinois (at least one in each county). When a birth is registered, the registrar retains one copy of this record, one copy is sent to the state, a microfilm copy is made and the original is sent to the state archives where it is bound. The information that is obtained for this registry includes date of birth, sex, race, parents' name, address, legitimacy and malformations.

The Vital Records Act places a legal restriction on the dissemination of this information. The person, if of legal age, can obtain a copy of his or her birth certificate upon written request and payment of a $2.00 fee. The birth record can also be obtained by court order. A record of illegitimate birth is impounded and can only be opened by court order.

The Office of Vital Records processes 500 daily requests for certified copies of birth records, and approximately 10,000 corrections per year. (An example is name spelling.) Adoptions and legitimizations total 12,000 a year, and in these cases a new birth record is created and the original is impounded.

Due to time constraints this test was limited to four hours for assessing value in terms of potential alteration or disclosure of information contained in the Birth Records System.

Estimating Information Value Based on Potential Disclosure

Two means are available for Birth Records information to be improperly exposed.

- Through normal channels
- Outside normal channels

The normal route of access to an individual's birth record is for the individual to submit a written request for a certified copy of his birth. If the requester falsely identifies himself, the Office of Vital Statistics "would not be liable for anything because the request must be in writing and there is no way of knowing that the request is false."

An example was given of a person in the Office of Vital Records disclosing to a friend the adoptive parents' name of the friend's illegitimate child. Another example involved disclosure of the illegitimate birth of a community leader by a local registrar to the local newspaper. To the custodian the "embarrassment or bad publicity" would have "some" impact on the organization. It might also result in loss of jobs for some administrators. Using the non-monetary dollarization scale shown earlier in this text, "some" is assessed as $25,000. Legally the discloser, not the Office of Vital Records, would be "guilty of a Class A misdemeanor.

The value of disclosure to the Subject of the information was considered. The reputation of the subject in the previous example was certainly affected. "If it were me, I'd sue for $1,000,000. That doesn't mean I'd get it." This aspect could have a "maximum" value. Certain disclosures could affect a subject's inheritance rights. An example of this would be to gain access to the original birth record to disinherit an adopted sibling. This example was related to the "insurance" value factor. The value was rated as "high", or $75,000.

Certain of these disclosure examples were determined to have a value to the intruder. The disclosure of an individual's illegitimacy while damaging to his or her reputation could be a political advantage to an intruder. There would be a gain in disinheriting a sibling for the other inheritors. Another aspect of value to the intruder was thought to be "Competitive Advantage." A list of the names and addresses of the parents of newborn babies would be very valuable to any business with a product or service geared to that market. Prior to the present restrictions on disseminating this particular information, "the going rate was five cents a name." In some areas names of these parents are printed in the local newspaper and in some cases both names and addresses are printed. In other areas this information is not made available to the public in a useable form. The competitive advantage would depend on the particular geographic area and the availability of this information. $50,000 was assessed as a realistic value for this factor.

The total value in terms of disclosure was assessed to be $500,000. ($250,000 each for intentional disclosure of computer media and human readable information.)

Estimating Information Value Based on Potential Alteration.

The "possibility of altering the Birth Records System source documents kept in the vault in the state archives is nearly nonexistent." If alteration could be accomplished, the impact would be "quite a bit" to the Office of Vital Records. The embarrassment alone or class action suit would have an impact at the "very top of the scale" or using the Utility Value conversion scale $100,000. An example of the value of altered information was given. Although in this instance the birth information is not actually altered at the source document level, the information as used is falsified or altered. There is a "black market in birth certificates." Briefly, a request is made for a copy of a birth certificate of someone (who is dead) as if the requestor were that person. These are sold to "illegal aliens for $500 to $600 each." Foreign powers use this same means to gain "citizen status" for spies. If the source information could be changed to negate the possibility of detecting the falsification, the value of the alteration would be "very, very tremendous." The value to the intruder of altered information is assessed in terms of being able to market a resource of citizenship — "hundreds of thousands of dollars."

The value to the Subject of altered birth information could also be assessed in terms of reputation and inheritance rights and the specific alteration value would be similar to the value as detailed under Disclosure.

The value in terms of alteration was assessed to be $1,550,000. ($775,000 each for accidental and intentional alteration.)

Summary of the test experience

The Administrator found little difficulty in estimating the various value factors for each exposure result. Initially estimating nonmonetary value was thought to be "impossible" but after explanation of the Utility Value dollar conversion scale the estimating was easily accomplished.

The benefit of evaluating the birth information system was described as "very important." "I see ignorance (of the value of this information) not only by the public but by the Department of Public Health. I see what you're trying to do." The security of this information is "a very important part affecting us, particularly in the future when all's on computer." It's important to explore this now rather than "jumping into it and cleaning up the hazards later."

When asked to describe the current information exposures the Administrator responded most unauthorized requests for information are "penny ante now." The phrase used is "I'll make it worth your while" and this happens about "twice a day." Due to the awareness of the staff in the Office of Vital Records of the confidentiality of this information there is a very small possibility of disclosure or alteration. "With the trend to computerize everything I see great impact. I see the computer as impersonal." There will be "one person only to bribe" and this will "open it up to the big leaguers" particularly in terms of information alteration.

CASE 2

Department of Public Health — Venereal Disease Information System

The Venereal Disease Information System is predominantly a manual system maintained by the Department of Public Health to support the Venereal Disease Treatment Program.

Estimating Information Value Based on Potential Destruction

"If all our information is destroyed — forget it" was the first reaction to estimating the cost of acquiring information which has been destroyed. This led to a discussion of the future value of this information. The loss of venereal disease records would necessitate extra field work in the future to determine disease history and treatment. By no means could they begin to "reconstruct" the lost historical information. That would be impossible. The value of the information in reference to past disease occurrences was assessed under the monetary utility, "Cost of Replacement." An estimate of eleven field workers for the first year was valued to be $50,000 to $60,000. The other value factors from the custodian viewpoint were not thought to be applicable.

"Action" or the "impact of the inability to act or perform mission" was judged to be of some value. The reprocessing necessary to regain the ability to act was estimated to cost $8,000 in extra help. The comment made about the value factor "Decision" implied that destruction would "impair our ability" to make a decision but that this value was covered under the "cost of replacement" estimate. The "lack of control" was defined as being the confusion cost incurred during an interim period, and was estimated without the scale to be $5,000. The value of the "loss of ability to account for operations" was discussed. The statistical information provides a basis for estimating grants and project monies needed. This ability was estimated as of some value but not really lost through the destruction of this information. There would be no legal implication as to the Department's authorization due to destruction of this information.

Value of destruction of the information from the subject's perspective was assessed from a utility standpoint. The only nonmonetary utility relevant was a subject's health or well-being. Loss of the medical history could mean a risk to the subject and also necessitate the start of treatment or testing again. This latter cost was estimated to be an average of $50 per subject, or a maximum total of $25,000 for the subjects on record.

The value of the intentional destruction of the information from the viewpoint of the intruder was considered. The publicity would be no greater than against any state facility or large organization, therefore, this factor was judged not applicable. The "value of secrecy" and "emotional satisfaction" were deemed the only intruder value factors that could be assessed, but they were judged to be of little value particularly because the information is not released in a form identifiable to an individual. The total value of information in terms of destruction was assessed to be $98,000.

Estimating the Value of Information Based on Potential Disclosure

Potential disclosure of the information was described as an "imagined abuse rather than anything real." The file of treated infected persons is not accurate because the history file contains outdated names and addresses. Thus, an intruder gaining the information for disclosure would have little chance of blackmail potential. There would be a very slim possiblity that "a person of importance" could be traced or identified because the diseased subject would seek treatment from a private physician not a Public Health Clinic, and would not be likely to use his or her real name. The consensus was that a successful Intruder intent on obtaining information for blackmail, would be sorely disappointed in that the information would have few, if any, blackmail possibilities. The value of information to the Intruder in terms of "emotional satisfaction" was estimated to be $1,000.

Because the venereal disease information could be identified with very few people, the value to the subject of disclosure was not considered to be high. It was described as a "loss of well-being to a very few people." First, the information would have to be identifiable to a subject, and second, that subject would have to be the type that considered disclosure harmful to his or her reputation. This was assessed as having "some" to "medium" value. Using the scale, $25,000 was assessed.

From the viewpoint of the Custodian, the administrators examined the value of disclosure of the information. In apparent contrast to the value assessment from the viewpoint of a subject, the first point discussed was the legal impact if disclosure took place. Given the lean of the courts an individual could get punitive damages "as high as the sky." A suit or the adverse publicity (which was considered the more likely result) would substantially impact the ability of the Public Health Department to carry out its health program against disease. The loss of public trust "would affect not only ours but every Public Health Program — well over $1 million in value" to regain public confidence. The criminal penalty would be a misdemeanor to the individual responsible and could mean loss of jobs to executives or others responsible, if such disclosure occurred through negligence on their part. The total value of information in terms of disclosure was assessed to be $1,026,000.

Estimating the Value of Information Based on Potential Alteration

Alteration was not considered a possibility because of the structure of the stored information, any alteration would be "so apparent it wouldn't be accepted."

Exposure Probability

The probability of exposure was assessed by MID personnel for the Birth Records System of the State of Illinois Department of Vital Records.

Exhibit G-1 shows the methodology used to assess the probability of exposure. The primary routes of access to information as shown on the exhibit are through remote site and local computer site locations. Within the remote and local site, access to information can feasibly be gained through the computer equipment, the operating system, and programs, and by physically accessing human and computer readable information in the various forms in which it is stored.

The rates of access were estimated by MID personnel based on forty-eight routes offered in the methodology. The number of attempts per timeframe were defined based on a logical estimate of the attempts to gain information which would be made within five years.

It should be noted that MID personnel did not have the experience to estimate the number of access attempts through the computer equipment, operating system or programming at remote sites. They did, however, estimate the attempts relative to human readable or computer media stored information at the remote site based on their knowledge of the remote site physical environment.

In using the methodology MID personnel considered the safeguards currently employed by MID and the Department of Vital Records and followed each route of access to information (i.e., through the physical site, computer equipment, operating systems, programming and information stored in human readable or computer media form) to determine the rate of accidental or intentional disclosure or alteration of information by insider (EDP) or outside personnel. The rate of destruction was not assessed due to time limitations.

Forty-eight individual routes of access are defined in the methodology and the rate of attempted access for each individual access route to the Birth Records is described in pages 2 and 5 of **Exhibit G-1.**

The rates (probability of exposure) estimated by MID personnel are used in Section 3 as input to the Total Expected Cost Model. It should be noted that the only routes of possible access were routes 2, 5, 6, 26 and 38.

EXPOSURE PROBABILITY

METHODOLOGY FOR DETERMINING LIKELIHOOD OF ATTEMPTED ACCESS TO INFORMATION

TIME FRAME FOR THE PROBABILITY 5 Years

TITLE OF INFORMATION SYSTEM BEING ASSESSED Birth Records System

RESULTS

ROUTE OF ATTEMPTED ACCESS (REMOTE PROCESSING SITE)	DISCLOSURE				ALTERATION				DESTRUCTION			
	INSIDER		OUTSIDER		INSIDER		OUTSIDER		INSIDER		OUTSIDER	
	ACCIDENTAL RATE	INTENTIONAL RATE	ACCIDENTAL RATE	INTENTIONAL RATE	ACCIDENTAL RATE	INTENTIONAL RATE	ACCIDENTAL RATE	INTENTIONAL RATE	ACCIDENTAL RATE	INTENTIONAL RATE	ACCIDENTAL RATE	INTENTIONAL RATE
1. PHYSICAL SITE												
REMOTE COMPUTER EQUIPMENT												
OPERATING SYSTEM												
PROGRAMMING												
HUMAN READABLE OR COMPUTER MEDIA INFORMATION	N	S	N	N	O	S	N	N				
2. PHYSICAL SITE (LOCAL PROCESSING SITE)												
LOCAL COMPUTER EQUIPMENT		S		N								
OPERATING SYSTEM		N		N								
PROGRAMMING		N		N								
HUMAN READABLE OR COMPUTER MEDIA INFORMATION	N	N	N	N	N	N	N	N				
3. PHYSICAL SITE												
COMPUTER MEDIA INFORMATION	N	S	N	N	N	N	N	N				
4. PHYSICAL SITE												
HUMAN READABLE INFORMATION	N	S	N	N	N	N	N	N				

CHOICES		NUMBER OF ATTEMPTS PER TIME FRAME	RATES AT ATTEMPTED ACCESS 1 YEAR	3 YEARS	5 YEARS
(N)	NEVER	0	0	0	0
(S)	SELDOM	1-3	2	2/3	2/5
(O)	OFTEN	4-8	6	2	6/5

INSTRUCTIONS:

(1) PICK TIME FRAME (1, 3 OR 5 YEARS).
(2) ESTIMATE NUMBER OF ATTEMPTS (YOU HAVE THREE CHOICES: NEVER (N), SELDOM (S), AND OFTEN (O). SEE ABOVE FOR DEFINITION OF THE CHOICES AND THE RESPECTIVE RATES OF ATTEMPTED ACCESS,).

EXHIBIT G-1
Page 1 of 5

The following access routes were assessed for the Birth Records System.

EXPLANATION OF ACCESS ROUTES

Description of Access	Access Route	Rate of Attempted Access
Human readable or computer media information - remote equipment		
1-4 Disclosure		
1-2 Insider		
1. Accidental	1	0
2. Intentional	2	0.4
3-4 Outsider		
3. Accidental	3	0
4. Intentional	4	0
5-8 Alteration		
5-6 Insider		
5. Accidental	5	1.2
6. Intentional	6	0.4
7-8 Outsider		
7. Accidental	7	0
8. Intentional	8	0
9-12 Destruction		
9-10 Insider		
9. Accidental	9	n.a.
10. Intentional	10	n.a.
11-12 Outsider		
11. Accidental	11	n.a.
12. Intentional	12	n.a.

Route Numbers
1 - 12

EXHIBIT G-1
Page 2 of 5

Route Numbers	Description of Access	Access Route	Rate of Attempted Access
13-24	Human readable or computer media information-local equipment		
	13-16 Disclosure		
	13-14 Insider		
	13. Accidental	13	0
	14. Intentional	14	0
	15-16 Outsider		
	15. Accidental	15	0
	16. Intentional	16	0
	17-20 Alteration		
	17-18 Insider		
	17. Accidental	17	0
	18. Intentional	18	0
	19-20 Outsider		
	19. Accidental	19	0
	20. Intentional	20	0
	21-24 Destruction		
	21-22 Insider		
	21. Accidental	21	n.a.*
	22. Intentional	22	n.a.
	23-24 Outsider		
	23. Accidental	23	n.a.
	24. Intentional	24	n.a.

Note: *n.a. = not available.

Route Numbers	Description of Access	Access Route	Rate of Attempted Access
25-36	Computer media information-local site		
	25-28 Disclosure		
	25-26 Insider		
	25. Accidental	25	0
	26. Intentional	26	0.4
	27-28 Outsider		
	27. Accidental	27	0
	28. Intentional	28	0
	29-32 Alteration		
	29-30 Insider		
	29. Accidental	29	0
	30. Intentional	30	0
	31-32 Outsider		
	31. Accidental	31	0
	32. Intentional	32	0
	33-36 Destruction		
	33-34 Insider		
	33. Accidental	33	n.a.
	34. Intentional	34	n.a.
	35-36 Outsider		
	35. Accidental	35	n.a.
	36. Intentional	36	n.a.

Route Numbers 37-48	Description of Access	Access Route	Rate of Attempted Access
	Human readable information-local site		
	37-40 Disclosure		
	37-38 Insider		
	37. Accidental	37	0
	38. Intentional	38	0.4
	39-40 Outsider		
	39. Accidental	39	0
	40. Intentional	40	0
	41-44 Alteration		
	41-42 Insider		
	41. Accidental	41	0
	42. Intentional	42	0
	43-44 Outsider		
	43. Accidental	43	0
	44. Intentional	44	0
	45-48 Destruction		
	45-46 Insider		
	45. Accidental	45	n.a.
	46. Intentional	n.a.	n.a.
	47-48 Outsider		
	47. Accidental	47	n.a.
	48. Intentional	48	n.a.

Identifying Safeguards, Cost and Reliability

Five safeguards were identified by MID personnel as appropriate to protect the information exposure access routes to the Birth Records System of the Office of Vital Records. The safeguards selected for use in the Total Expected Cost Model include:

- Software Audit Trail at the Remote Location.
- Hardware and Personnel Verification Checking at the Remote Location.
- Software Authorization Checking at the Remote Location.
- Exit Control of Personnel at MID.
- Hardware and Personnel Surveillance at MID.

The specific use of these safeguards in the TEC Model is explained in Section 4.

APPENDIX H

This Appendix contains a development of the Total Expected Cost Model presented in Chapter IV of the text for determining the best system for securing the resources of a data processing center. It relies upon a knowledge of the vocabulary and definitions given in earlier sections. Appendix H is divided into three parts.

- The first defines symbols, states the mathematical model, and lists assumptions.
- The second explains the construction of the model, discusses the assumptions which must be made in order to use, and gives a more detailed explanation of the example calculations made in the text.
- The third extends the model so that it can be used for a planning period longer than one year and gives the example of Chapter IV assuming a five year planning period.

Model and Assumptions

Let

$v_{j\ell}$ = value of the jth resource if exposed via the ℓ th exposure access route, j = 1, 2, ..., m, ℓ = 1, 2, ..., 48.

$\lambda_{j\ell}$ = average number of times per year someone attempts to expose jth resource via the ℓ th exposure access route, j = 1, 2, ..., m, ℓ = 1, 2, ..., 48.

c_i = cost of ith safeguard, i = 0, 1, 2, ..., n.

$q_{ij\ell}$ = conditional probability the ith safeguard does **not** prevent exposure of the jth resource, given there is an attempt to expose the jth resource via the ℓ th exposure access route, i = 0, 1, 2, ..., n, j = 1, 2, ..., m, ℓ = 1, 2, ..., 48.

The symbols X_k, XI_k, XO_k, Y_k and TEC_k will also be used. These have been previously defined.

Following is a summary of the indices which are being used:

i is a safeguard,

j is a resource (information) contained in the data processing center,

k is a security system (a collection of 0, 1, 2, or more safeguards), and

ℓ is an exposure access route.

The mathematical model for determining the total expected cost (TEC_k) for security system k is:

$$TEC_k = X_k + Y_k,$$

where * $$X_k = \sum_{i \in k} c_i = XI_k + XO_k,$$

$$Y_k = \sum_{j=1}^{m} \sum_{\ell=1}^{48} v_{j\ell} \lambda_{j\ell} r_{jk\ell},$$

and where $r_{jk\ell} = \prod_{i \in k} q_{ij\ell}$.

Following are the assumptions which must be made in order to use this model:

- The number of attempted exposures per year of a given resource is a random variable which has a Poisson probability distribution.
- The following data relative to the solution of this problem can be obtained:

  Cost of potential safeguards,
  Reliability of potential safeguards,
  Value of the information being secured, and
  Average number of attempts per year to expose a given type of information.

  Realize that the exact values for most of this data are unknown; however, Chapter IV of the text presents a methodology for estimating them.

- Safeguards work independently of each other, that is, if two safeguards are employed to secure the same information, the success or failure of one is independent of the success or failure of the other.
- The installation of a safeguard will not eliminate attempts at exposing information, just their probability of success.

Before proceeding, if you are not accustomed to the concept of expected loss you should consider what it means from a probabilistic point of view. The loss due to exposure of information is a random variable. The expected loss, a single number, is used by the model to characterize this random variable and its probability distribution. If we were able to obtain a random sample of the loss due to exposure, then the arithmetic mean of the sample would approach the expected value of the loss as the sample size increased. However, it must be noted that the real loss due to exposure could take on many values — some larger than its expected value and some smaller. In other words, the real loss may be many times larger or smaller than this expected value.

*X_k is found by summing the costs of the safeguards comprising security system k. In some cases, however, safeguards share costs (see example, Chapter IV), and X_k cannot be found by simply summing the c_i for all i belonging to k. For reasons which will be clear in the third part of this Appendix, X_k is divided into the two components, XI_k and XO_k.

Construction of the Model

This section is devoted to developing and explaining the expected loss (Y_k) portion of the total expected cost (TEC_k) model. The cost to install and operate safeguards (X_k), has been treated previously.

Let $Z_{j\ell}$ = number of attempted exposures per year of resource j via exposure access route ℓ.

Clearly, $Z_{j\ell}$ is a discrete random variable. It is assumed that $Z_{j\ell}$ follows a Poisson probability distribution with parameter $\lambda_{j\ell}$, i.e., $\lambda_{j\ell}$ is the average number of attempted exposures per year of resource j via exposure access route ℓ. Using the Poisson distribution assumes that the exposure process is memoryless, i.e., the number of attempted exposures in the time interval (t_1, t_2) is independent of the number of attempted exposures in a subsequent time interval (t_2, t_3). In many cases this is not a bad assumption because, unlike the security problems of a bank, most successful attempts to access a resource contained in a data processing center will go undetected.

The purpose of the model is to find the most cost-effective mix of safeguards which should be employed over a given period of time, the decision period. In the example in Chapter IV of the text, the decision period was one year; however, it could be any length of time and due to the high implementation costs of some safeguards, the decision period is more likely to be three to five years in duration. The model assumes a static environment exists during the decision period, i.e., $\lambda_{j\ell}$ remains constant over this period, regardless of the safeguards employed or the detection achieved. This implies that when a successful or unsuccessful attempted exposure is uncovered, you do not rush out and purchase more security to protect that exposure access route. In reality, the security of a data processing center is dynamic. When you uncover an attempted exposure, you would tend to plug future possible exposures via that access route. However, based upon the available data it is not certain that very many attempted exposures will come to your attention.

We are now ready to develop the method for finding the expected loss per year due to exposure of resources. To simplify the following discussion, assume we are dealing with only one resource, one exposure access route, and one safeguard. This allows us to drop the subscripts i, j, k, and ℓ for the moment.

Let v = value of the resource,

Z = number of attempted exposures per year of the resource,

λ = average number of attempted exposures per year of the resource,

r = conditional probability the safeguard does **not** prevent exposure of the resource, given an attempt is made to expose it, and

Y = expected loss per year due to exposure of the resource.

Consider the following two events:

Event A = an attempted exposure of the resource occurs, and
Event B = the resource is exposed.
If P (x) = probability that event x occurs.

Then,

Expected Loss = $v \cdot P(A \cap B) = v \cdot P(A)P(B/A)$.

This expression illustrates the basic model for the expected loss due to exposure and the type of data that is necessary in order to determine this loss. It does not take into account, however, the fact that there can be more than one attempted exposure per year. The following model does:

$$\begin{aligned} Y &= v \cdot P(Z=1) \cdot r + 2v \cdot P(Z=2) \cdot r + 3v \cdot P(Z=3) \cdot r + \cdots \\ &= v \left\{ P(Z=1) + 2P(Z=2) + 3P(Z=3) + \cdots \right\} r \\ &= v\, E(Z) r = v \lambda r, \end{aligned}$$

where $P(B/A) = r$.

Now suppose there is more than one safeguard securing this resource. In this case, suppose there are exactly two safeguards.

Let q_1 = conditional probability the 1st safeguard does **not** prevent exposure of the resource, given an attempt is made to expose it.

q_2 = conditional probability the 2nd safeguard does **not** prevent exposure of the resource, given an attempt is made to expose it.

An attempt to expose the resource is successful only if both safeguards fail to protect it. Assuming that both safeguards work independently of each other,

$$P(B/A) = r = q_1 \cdot q_2$$

The model generalizes quite easily to cover m resources, each of which can be exposed via different access routes. For 2, 3, ..., m resources, we apply the same model and sum the expected loss over all resources; hence, introducing subscript j,

$$Y = \sum_{j=1}^{m} v_j \lambda_j r_j.$$

For 2, 3, ..., 48 possible exposure access routes (we have identified 48; however, others could easily be identified and incorporated into the model), we expand the same model and sum the expected loss over all exposure access routes; hence, introducing subscript ℓ,

$$Y = \sum_{j=1}^{m} \sum_{\ell=1}^{48} v_{j\ell} \lambda_{j\ell} r_{j\ell}.$$

Finally, to compare different security systems, each composed of a different mix of safeguards, we introduce the subscript k and have,

$$Y_k = \sum_{j=1}^{m} \sum_{\ell=1}^{48} v_{j\ell} \lambda_{j\ell} r_{jk\ell}.$$

In this final model, the value of resources and the average number of attempts per year to expose them are assumed to be independent of the security system, k. However, the probability the safeguards do not prevent exposure, given an attempt is made, is not independent of the security system.

Following the reasoning and assumption presented above in the case of two safeguards,

$$r_{jk\ell} = \prod_{i \in k} q_{ij\ell}$$

= the product of the $q_{ij\ell}$ for all safeguards i comprising security system k.

By having $\lambda_{j\ell}$ independent of k in this model, it is assumed that the installation of a safeguard will not reduce or eliminate attempts at exposing a resource, just their probability of success. This assumption can be relaxed quite easily by making the average number of attempted exposures per year of resource j via exposure access route ℓ dependent upon the safeguards comprising security system k. This requires replacing $\lambda_{j\ell}$ with $\lambda_{jk\ell}$ in the above model. Doing this recognizes the possibility that safeguards have a deterrent effect on attempted exposures.

This part concludes with some example calculations to illustrate how the TEC_k of a security system are obtained, using the data given previously.

TEC_0:

$X_0 = 0$ No new safeguards are employed; hence, there is no new cost in providing security

$$Y_0 = \sum_{j=1}^{1} \sum_{\ell=1}^{48} v_{j\ell} \lambda_{j\ell} r_{j,0,\ell}$$

$$= v_{1,2} \lambda_{1,2} r_{1,0,2} + v_{1,5} \lambda_{1,5} r_{1,0,5} + v_{1,6} \lambda_{1,6} r_{1,0,6} + v_{1,26} \lambda_{1,26} r_{1,0,26} + v_{1,38} \lambda_{1,38} r_{1,0,38}.$$

$r_{1,0,\ell} = \prod_{i \in 0} q_{i,1,\ell}$ The only safeguard used in security system 0 is i = 0, hence

$r_{1,0,\ell} = q_{0,1,\ell} = 1.00$, for $\ell = 2, 5, 6, 26, 38.$

Therefore, using the data from the previous exhibit,

$$Y_0 = 100{,}000(1.00) + 930{,}000(1.00) = 310{,}000(1.00) + 100{,}000(1.00) + 100{,}000(1.00)$$

$$= \$1{,}540{,}000.$$

$$TEC_0 = X_0 + Y_0 = 0 + 1{,}540{,}000 = \$1{,}540{,}000.$$

TEC_1:

$$X_1 = c_1 = XI_1 + XO_1 = \$10{,}000 + 6{,}000 = \$16{,}000.$$

$$Y_1 = \sum_{J=1}^{1} \sum_{\ell=1}^{48} v_{j\ell}\ \lambda_{j\ell}\ r_{j,1,\ell}$$

$$= v_{1,2}\,\lambda_{1,2}\,r_{1,1,2} + v_{1,5}\,\lambda_{1,5}\,r_{1,1,5} + v_{1,6}\,\lambda_{1,6}\,r_{1,1,6} + v_{1,26}\,\lambda_{1,26}\,r_{1,1,26} + v_{1,38}\,\lambda_{1,38}\,r_{1,1,38}.$$

$r_{1,1,\ell} = \prod_{i \in 1} q_{i,1,\ell}$. The only safeguard used in security system 1, is i = 1, hence

$$r_{1,1,\ell} = q_{1,1\ell}, \text{ for } \ell = 2, 5, 6, 26, 38.$$

From the exhibit, $q_{1,1,2} = q_{1,1,6} = .05$ and $q_{1,1,5} = q_{1,1,26} = q_{1,1,38} = 1.00$.

Therefore, using these values for $r_{1,1,\ell}$ and the data from the exhibit,

$$Y_1 = 100{,}000(.05) + 930{,}000(1.00) + 310{,}000(.05) + 100{,}000(1.00) + 100{,}000(1.00)$$

$$= \$1{,}150{,}500.$$

$$TEC_1 = X_1 + Y_1 = 16{,}000 + 1{,}150{,}500 = \$1{,}166{,}500.$$

TEC_6:

$$X_6 = c_1 + c_2 = (10{,}000 + 6{,}000) + (2{,}000 + 6{,}900)$$

$$= (10{,}000 + 2{,}000) + (6{,}000 + 6{,}900)$$

$$= 12{,}000 + 12{,}900 = XI_6 + XO_6$$

$$= \$24{,}900.$$

$$Y_6 = \sum_{j=1}^{1} \sum_{\ell=1}^{48} v_{j\ell}\ \lambda_{j\ell}\ r_{j,6,\ell}$$

$$= v_{1,2}\,\lambda_{1,2}\,r_{1,6,2} + v_{1,5}\,\lambda_{1,5}\,r_{1,6,5} + v_{1,6}\,\lambda_{1,6}\,r_{1,6,6} + v_{1,26}\,\lambda_{1,26}r_{1,6,26} + v_{1,38}\,\lambda_{1,38}r_{1,6,38}.$$

$r_{1,6,\ell} = \prod_{i \in 6} q_{i,1,\ell}$. There are two safeguards composing system 6, i = 1 and 2, hence

$r_{1,6,\ell} = q_{1,1,\ell} \cdot q_{2,1,\ell}$, for ℓ = 2, 5, 6, 26, 38.

Using the values for $q_{ij\ell}$ from the exhibit,

$$r_{1,6,2} = q_{1,1,2} \cdot q_{2,1,2} = .05(1.00) = .05$$

$$r_{1,6,5} = q_{1,1,5} \cdot q_{2,1,5} = 1.00(.02) = .02$$

$$r_{1,6,6} = q_{1,1,6} \cdot q_{2,1,6} = .05(1.00) = .05$$

$$r_{1,6,26} = q_{1,1,26} \cdot q_{2,1,26} = 1.00(1.00) = 1.00$$

$$r_{1,6,38} = q_{1,1,38} \cdot q_{2,1,38} = 1.00(1.00) = 1.00$$

Therefore, using these values for $r_{1,6,\ell}$ and the data from the exhibit,

$$Y_6 = 100{,}000(.05) + 930{,}000(.02) + 310{,}000(.05) + 100{,}000(1.00) + 100{,}000(1.00) = \$239{,}100.$$

$$TEC_6 = X_6 + Y_6 = 24{,}900 + 239{,}100 = \$264{,}000.$$

TEC_{30}:

$$X_{30} = c_2 + c_3 + c_4 + c_5$$

Note, however, that safeguards 4 and 5 both use guards at the local site and these guards perform both exit control and surveillance. Therefore, the operating cost and some implementation cost for these two safeguards is a shared cost and must not be duplicated.

$$= (2{,}000 + 6{,}900) + (50{,}000 + 36{,}000) + (6{,}000 + 60{,}000) + (10{,}000 + 0)$$

$$= (2{,}000 + 50{,}000 + 6{,}000 + 10{,}000) + (6{,}900 + 36{,}000 + 60{,}000 + 0)$$

$$= 68{,}000 + 102{,}900 = XI_{30} + XO_{30}$$

$$= \$170{,}900.$$

$$Y_{30} = \sum_{j=1}^{1} \sum_{\ell=1}^{48} v_{j\ell} \lambda_{j\ell} r_{j,30,\ell}$$

$$= v_{1,2} \lambda_{1,2} r_{1,30,2} + v_{1,5} \lambda_{1,5} r_{1,30,5} + v_{1,6} \lambda_{1,6} r_{1,30,6} + v_{1,26} \lambda_{1,26} r_{1,30,26} + v_{1,38} \lambda_{1,38} r_{1,30,38}.$$

$r_{1,30,\ell} = \prod_{i \in 30} q_{i,1,\ell}$. There are four safeguards composing system 30, i = 2, 3, 4, and 5, hence

$r_{1,30,\ell} = q_{2,1,\ell} \cdot q_{3,1,\ell} \cdot q_{4,1,\ell} \cdot q_{5,1,\ell}$, for ℓ = 2, 5, 6, 26, 38.

Using the values for $q_{ij\ell}$ from the exhibit,

$r_{1,30,2} = q_{2,1,2} \cdot q_{3,1,2} \cdot q_{4,1,2} \cdot q_{5,1,2} = 1.00(.00)\ (1.00)\ (1.00) = .00$

$r_{1,30,5} = q_{2,1,5} \cdot q_{3,1,5} \cdot q_{4,1,5} \cdot q_{5,1,5} = .02(1.00)\ (1.00)\ (1.00) = .02$

$r_{1,30,6} = q_{2,1,6} \cdot q_{3,1,6} \cdot q_{4,1,6} \cdot q_{5,1,6} = 1.00(.00)\ (1.00)\ (1.00) = .00$

$r_{1,30,26} = q_{2,1,26} \cdot q_{3,1,26} \cdot q_{4,1,26} \cdot q_{5,1,26} = 1.00\ (1.00)\ (.02)\ (.30) = .006$

$r_{1,30,38} = q_{2,1,38} \cdot q_{3,1,38} \cdot q_{4,1,38} \cdot q_{5,1,38} = 1.00(1.00)\ (.02)\ (.30) = .006$

Therefore, using these values for $r_{1,30,\ell}$ and the data from the exhibit,

$$Y_{30} = 100{,}000(.00) + 930{,}000(.02) + 310{,}000(.00) + 100{,}000(.006) + 100{,}000(.006)$$

$$= 0 + 18{,}600 + 0 + 600 + 600 = \$19{,}800.$$

$$TEC_{30} = X_{30} + Y_{30} = 170{,}900 + 19{,}800 = \$190{,}700.$$

Extended Planning Period

Because of the high implementation costs of most safeguards, the determination of the best system for securing the contents of a data processing center will generally be based on comparing the total expected costs of alternative systems over a period of from three to five years. The purpose of this section is to show how the model presented above can be used, with slight revision, to take into account a planning period greater than one year.

The revised model is:

$$TEC_k = XI_k + PWF(XO_k + Y_k),$$

where TEC_k = present worth of total expected costs of security system k over the planning period, and PWF = present worth factor.

This model separates the costs XO_k and Y_k, which recur each year of the planning period, from the costs XI_k, which occurs only when the safeguards comprising system k are installed, that is, during the first year of the planning period. Using the present worth factor (PWF), all future costs (real or expected) are adjusted to their present worth at the beginning of the planning period, for purposes of comparison.

The PWF depends upon the interest rate selected and the length of the planning period. Using a planning period of five years and an interest rate of 10%, this model can now be used to determine the best security system for the example problem presented in Chapter 4. In this case the PWF = 3.791. The resulting calculations appear in Exhibit H-1, which gives the XI_k, XO_k, and Y_k for each non-redundant security system and TEC_k for the undominated systems. Security system 28 appears to be the best system, if used over a five year period; however, the total expected cost of system 17 is only $615 greater than the cost of system 28, so it is really a toss-up between the two systems.

EXHIBIT H-I

SECURITY SYSTEM k	SAFEGUARDS COMPRISING K	XI_k ($)	XO_k ($/YR)	Y_k ($/YR)	$XO_k = Y_k$ ($/YR)	$PWF(XO_k + Y_k) = 3.791(XO_k + Y_k$ ($)	TEC_k ($)
0	0	0	0	1,540,000	1,540,000	5,838,140	5,838,140
1	1	10,000	6,000	1,150,500	1,156,500		
2	2	2,000	6,900	628,600	635,500	2,409,181	2,411,181
3	3	50,000	36,000	1,130,000	1,166,000		
4	4	6,000	60,000	1,342,000	1,402,000		
5	5	16,000	60,000	1,400,000	1,460,000		
6	1,2	12,000	12,900	239,100	252,000	955,332	967,332
7	1,3						
8	1,4	16,000	66,000	954,500	1,020,500		
9	1,5	26,000	66,000	1,010,500	1,076,500		
10	2,3	52,000	42,900	218,600	261,500		
11	2,4	8,000	66,900	432,600	499,500	1,893,605	1,901,605
12	2,5	18,000	66,900	488,600	555,500		
13	3,4	56,000	96,000	934,000	1,030,000		
14	3,5	66,000	96,000	990,000	1,086,000		
15	4,5	16,000	60,000	1,341,200	1,401,200		
16	1,2,3						
17	1,2,4	18,000	72,900	43,100	116,000	439,756	457,756
18	1,2,5	28,000	72,900	99,100	172,000		
19	1,3,4						
20	1,3,5						
21	1,4,5	26,000	66,000	951,700	1,017,700		
22	2,3,4	58,000	102,900	22,600	125,500		
23	2,3,5	68,000	102,900	78,600	181,500		
24	2,4,5	18,000	66,900	429,800	496,700		
25	3,4,5	66,000		931,200	1,027,200		
26	1,2,3,4						
27	1,2,3,5						
28	1,2,4,5	28,000	72,900	40,300	113,200	429,141	457,141
29	1,3,4,5						
30	2,3,4,5	68,000	102,900	19,800	122,700		
31	1,2,3,4,5						

END