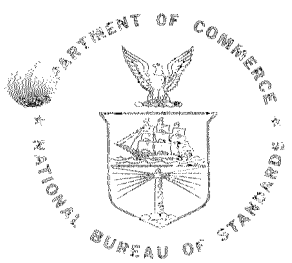
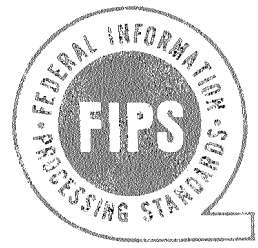


FIPS PUB 65

FEDERAL INFORMATION
PROCESSING STANDARDS PUBLICATION

1979 AUGUST 1

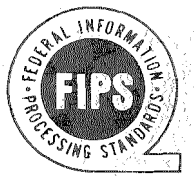
U.S. DEPARTMENT OF COMMERCE / National Bureau of Standards



Guideline

FOR AUTOMATIC DATA PROCESSING RISK ANALYSIS

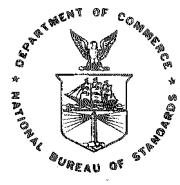
CATEGORY: ADP OPERATIONS
SUBCATEGORY: COMPUTER SECURITY



Federal Information Processing Standards Publication 65

1979 August 1

ANNOUNCING THE



GUIDELINE FOR AUTOMATIC DATA PROCESSING RISK ANALYSIS

Federal Information Processing Standards Publications are issued by the National Bureau of Standards pursuant to the Federal Property and Administrative Services Act of 1949, as amended, Public Law 89-306 (79 Stat. 1127), Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 Code of Federal Regulations (CFR).

Name of Guideline. Guideline for Automatic Data Processing Risk Analysis.

Category of Guideline. ADP Operations, Computer Security.

Explanation. This Guideline explains the reasons for performing a risk analysis, details the management involvement necessary and presents procedures and forms to be used for risk analysis and cost effective evaluation of safeguards.

Approving Authority. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Maintenance Agency. Department of Commerce, National Bureau of Standards (Institute for Computer Sciences and Technology).

Cross Index.

a. Federal Information Processing Standards Publication (FIPS PUB) 31, Guidelines for Automatic Data Processing Physical Security and Risk Management.

b. Federal Information Processing Standards Publication (FIPS PUB) 39, Glossary for Computer Systems Security.

c. Federal Information Processing Standards Publication (FIPS PUB) 41, Computer Security Guidelines for Implementing the Privacy Act of 1974.

d. Federal Information Processing Standards Publication (FIPS PUB) 46, Data Encryption Standard.

e. Federal Information Processing Standards Publication (FIPS PUB) 48, Guidelines on Evaluation of Techniques for Automated Personal Identification.

Applicability. This Guideline is applicable to all Federal agencies required to take action under the Office of Management and Budget Circular A-71, Transmittal Memorandum No. 1 of July 27, 1978, to ensure an adequate level of security for agency data.

Implementation. This Guideline should be referenced in the formulation of plans by Federal agencies for performing a risk analysis, whether or not the analysis is to be carried out by agency personnel or on contract.

Specifications. Federal Information Processing Standard 65 (FIPS PUB 65), Guideline for Automatic Data Processing Risk Analysis (affixed).

Qualifications. This Guideline has been prepared in order that a technique may be available for Federal agencies desiring to use it. However, it has become apparent that risk analysis technology is still in the evolutionary phase. As such, its further development would be seriously impeded by the establishment of a Federal risk analysis standard which required all agencies to adopt exactly the same methodology. Nevertheless, the needs of the Federal Government can only be met by the performance of risk analyses. Bearing in mind the pressure of both of these thrusts, the National Bureau of Standards is conducting an effort to identify the necessary constituent factors of risk analysis. With these established in a standard, Federal agencies will be able to conduct, or to have conducted for them, risk analyses with high confidence in the reliability of the product. On the other hand, research in the area will not be deterred by the inflexibility of an already prescribed methodology but should be encouraged by the setting of basic criteria and the challenge of developing and refining more sophisticated and more easily applied techniques.

Where to Obtain Copies of the Guideline. Copies of this publication are for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, Virginia 22161. When ordering, refer to Federal Information Processing Standards Publication 65 (NBS-FIPS-PUB-65) and title. When microfiche is desired, this should be specified. Payment may be made by check, money order, or deposit account.

Acknowledgment

The procedure for risk analysis presented here is based on the work of Robert H. Courtney, Jr. of the IBM Corporation, who, while a member of the Federal Information Processing Standards Task Group on Computer Systems Security, gave his kind permission for its adaptation to the needs of the Federal Government.

Appreciation is also expressed to those other members of the Task Group who contributed innovative and imaginative ideas to the development of this Guideline.

Federal Information
Processing Standards Publication 65

1979 August 1

SPECIFICATIONS FOR

GUIDELINE FOR AUTOMATIC DATA PROCESSING RISK ANALYSIS

CONTENTS

1. INTRODUCTION

Hand in hand with the increase in awareness of the need for computer security has come the need for a method of quantifying the impact of potential threats on organizations supported by automatic data processing. Risk analysis is such a method. It looks at an organization's ability to perform its missions and tasks correctly and in a timely manner under conditions which can affect physical environment, personnel, equipment, content of files and processing capability in conjunction with the chances for such conditions taking place.

There are any number of techniques for performing such analyses but two key elements must always be considered:

1. The damage which can result from an event of an unfavorable nature.

2. The likelihood of such an event occurring.

The aim of a risk analysis is to help ADP management strike an economic balance between the impact of risks and the cost of protective measures. It serves to point out the risks which exist; the required protective measures are then selected accordingly. An analysis shows the current security posture of ADP processing in an organization; it then assembles the basic facts necessary for the selection of adequate, cost effective safeguards. A secondary benefit of a risk analysis is the increased security awareness which will be apparent at all organizational levels, from management through operations.

A risk analysis provides management with information on which to base decisions, e.g., whether it is best to prevent the occurrence of a situation, to contain the effect it may have, or simply to recognize that a potential for loss exists. Because a risk analysis is the basis for such decisions, its estimates of loss or damage must be presented, where possible, in a quantitative, comparative fashion.

There are a number of other methods of inspecting, testing or evaluating the security of computer systems, such as penetration attempts, security audits, checklists and questionnaires. However, none of them can take the place of a risk analysis because their purposes are different and they do not consider the key elements of damage and likelihood of occurrence.

Risk analysis is not a task to be accomplished once for all time. It must be performed periodically in order to stay abreast of changes in mission, facilities and equipment. And since security measures designed at the inception of a system have generally proved to be more effective than those superimposed later, risk analysis should have a place in the design phase of every system.

The major resource required for a risk analysis is manpower—highly skilled manpower. For this reason the first analysis will be the most expensive, as subsequent ones can be based in part on previous work and the time required will decrease to some extent as expertise is gained.

The time allowed to accomplish the risk analysis should be compatible with its objectives. Large facilities with complex, multi-shift operations and many files will require more time to complete than single-shift, limited production facilities. If meaningful results are expected, management must be willing to commit the resources necessary for accomplishing this undertaking.

2. THE ROLE OF MANAGEMENT

2.1 Management

The success of risk analysis depends on the role top management takes in the project. There must be

1. management support of the project expressed to all levels of the organization;
2. management explanation of the purpose and scope of risk analysis;

3. management selection of qualified team and formal delegation of authority and responsibility; and

4. management review of the team's findings.

Management should leave no doubt that it intends to rely on the findings of the risk analysis team. The scope of the project should be defined to encompass ADP users (this will probably include all departments and any users outside the organization) as well as the actual ADP facility, equipment and personnel.

2.2 Risk Analysis Team

The selection of the risk analysis team is critical to the outcome of the project. It is important to obtain representation from the organizational components responsible for the following:

ADP operations management
Systems programming (if separate from ADP operations)
Internal auditing
Physical security
Data files under consideration
(Very probably, all the applications processed by the facility will not be the responsibility of the same organizational component; in that case, a component need only be represented when its own data files are being considered.)
Programming support of the files under consideration.

These entities should be represented on the team by people who are well informed both of their own component's mission and its relationship to the overall organizational mission. The task team leader should be equally knowledgeable and should come from one of the first three components listed above, but should not be that component's representative. In other words, the team leader should not wear two hats—one as leader and one as representative. None of this should be construed as precluding others from participation on the team and, certainly, departments such as legal and personnel should at least be consulted.

The leader and the team members should be designated in writing; their duties, responsibilities and any accompanying authority should be outlined. It should also be understood that the job cannot be done adequately if alternates are assigned. There may be a tendency on the part of the team members, in an effort to do a thorough job, to collect more information than is absolutely necessary; they should be cautioned about this as it can prolong the task.

There are reliable commercial firms which perform risk analyses on contract. It may be that management will decide to select one of them in preference to performing the task internally. That option should not be chosen in lieu of understanding the purpose and techniques of risk analysis, but rather in the interest of efficient resource utilization. The individuals who should serve on a risk analysis team are the same ones who will be needed to supply information to the contractor and to make certain that the product is a risk analysis rather than a list of vulnerabilities together with a list of intuitively chosen solutions. Although organization members could devote somewhat less time to it, especially in an organization maintaining a large number of applications systems and supporting files, they should still be readily available to the contractor throughout the risk analysis.

2.3 Allocation of Time

Risk analysis is a time-consuming process and one which cannot be hastened. Previous experience or a previous risk analysis to refer to will help considerably as will having all the necessary information readily available. At best, the consideration of each data set or file in the light of the hazards which beset a system is a tedious business, but one which should only be delegated to subordinates with great deliberation because of the level of knowledge and experience required in the decision process. It can be a very enlightening task, however, and one which may lead to system simplification.

The assignment of some individuals to the team may create a hardship for their organizational components, which will be forced to do without their services, as well as on the team members, who will feel compelled to rush through the risk analysis to get back to their

normally assigned duties. An agreement that the team will meet only half of each day would alleviate some of these burdens.

2.4 Management Review

Top management should review both the preliminary findings and the final results of the risk analysis team for reasonableness, policy adherence and organizational unity before a protection plan is formulated. At the very least, the plan will require coordination with fiscal and administrative departments, and will probably be included in the organization's long-range planning.

3. PRELIMINARY SECURITY EXAMINATION

In order to have a firm basis for conducting a risk analysis, the team should initiate the project by surveying the organization's existing ADP security, the cost of replacing assets, and the actual threats to which the organization's ADP processing is vulnerable. They will gain knowledge from the survey which may somewhat reduce the amount of time required for the risk analysis. The natural inertia of getting started in such a group is easily overcome because of the three specific products that are required from this preliminary phase—the list of assets replacement costs, the list of threats to which the facility is actually vulnerable, and the list of existing security measures.

3.1 Asset Costs

One product of the examination should be a list of the replacement costs, or best estimates thereof, of resources and facilities: the computer(s), related equipment, data, buildings, etc. The total of all should be noted. Better than any other information available at this time, this figure will give an indication of the need for security. If the risk analysis is being done in the system design phase, both the increased value of data in the completed system and the probable increase in the cost of acquiring it should be considered.

3.2 Threats

Another product of the preliminary phase should be a list of the actual threats to which the ADP facility and its resources are exposed. For instance, the occurrence of a tornado is a real possibility in the interior plains; in most coastal regions it is only a very remote possibility. Identifying the actual threats will give the risk analysis team a feel for the vulnerabilities, or possibilities for damage, of the facility and the systems they will be analyzing. Again, if the risk analysis is being done in the system design phase, an effort should be made not only to identify existing threats but to predict any future ones which might result from the implementation or operation of the system. The areas in the organization which should be surveyed for this purpose include:

- Personnel—hiring and termination procedures, scope and amount of training, quality of supervision at all levels.
- Physical Environment—neighborhood, quality and reliability of utilities, building design, operation and maintenance, physical access controls.
- Hardware/Software Systems—operational availability, change controls, software features, documentation.
- Data Communications — hardware and transmission circuits, procedures to validate and control distribution of messages.
- ADP Applications—technical design, documentation, standards. (Also see Appendix A.)
- Operations—standards and procedures for source document protection, information

dissemination, I/O control, tape library, forms, computer room processing, user interface, housekeeping and maintenance, production control, contingency planning.

Understanding the factors which contribute to system vulnerability is important in performing a risk analysis. These factors are hardly ever discrete and unrelated. Below is a sketchy example of the kind of approach which can be used to ferret out vulnerabilities.

- Natural Disasters. What kinds of natural disasters might reasonably be expected to occur? To what extent will the facility, processing availability, data, supplies, utilities, local transportation, etc., be affected?

- Environment. What special hazards such as explosives, flammable products, unused or unguarded buildings are nearby? What can be the aftermath of a fire in the vicinity? What is the proximity of the fire department?

- Facility Housing. Is ADP facility the sole occupant of the building? If not, what others? By whom is the building administered? By whom maintained? What construction is it? What warning devices and preventative equipment are installed? How close is it to heating equipment, cooking equipment, other fire hazards? What kind of floors and ceilings are there?

- Access. Is access to processing local or remote? Can an intruder gain access to processing, to data, to software, to equipment, to storage media, to preprinted forms, to supplies, to documentation, to output, to trash? Can an employee do the same? Accidentally? Maliciously? For profit?

- Work Scene. Is employee/management relationship satisfactory? How well do supervisors know personnel? Does management understand problems of personnel on shifts? How well do supervisors relay employee problems to management? Are employees loyal?

- Data Value. How much can an intruder gain by penetrating the system or disclosing data or disrupting operations? How much can a subject be hurt by unauthorized disclosure of data or by incorrect data? How much can the organization be hurt by disclosure of data or by basing decisions on incorrect data or by delayed processing availability?

3.3 Existing Security Measures

The last product of this phase should be a list of all security safeguards currently in effect, whether or not the original purpose of such features (e.g., storage media logs, control of printout distribution, data entry quality controls) was to protect. It will in fact be seen that good management practices generally promote security. Specific security measures, such as perimeter fences, guards, entrance badges, etc., may be for the protection of all offices and facilities in the building and would be in place even if the ADP facility were located elsewhere. The threats against which each of these in-place measures is specific should also be listed.

3.4 Management Review

The results of these surveys should be presented to management immediately upon completion. These results may point to the need for temporary safeguards until a final security plan, based on a complete risk analysis, can be placed in effect.

4. RISK ANALYSIS

Regardless of the cause, any harm which occurs in automatic data processing manifests itself as a loss to the organization of one, or more, of the following conditions:

DATA INTEGRITY—The state that exists when automated data is the same as that in the source documents, or has been correctly computed from source data, and has not been

exposed to accidental alteration or destruction. Incomplete data, unauthorized changes or additions to the data, and erroneous source data are all considered violations of data integrity.

DATA CONFIDENTIALITY—The state that exists when data is held in confidence and is protected from unauthorized disclosure. Misuse of data by those authorized to use it for limited purposes only is also considered to be a violation of data confidentiality.

ADP AVAILABILITY—The state that exists when required ADP services can be performed within an acceptable time period even under adverse circumstances.

To prevent the risk analysis from bogging down in detail, the team should concentrate on the potential results of undesirable events, i.e., on the extent of the damage which they can cause, rather than on why they occur since the harmful events to which the organization is vulnerable have already been identified in the preliminary phase.

4.1 Elements

The essential elements of risk analysis are an assessment of the damage which can be caused by an unfavorable event and an estimate of how often such an event may happen in a period of time.

As it will be impossible for the team to know absolutely either the impact or frequency of many events, these must be estimated using a combination of historical data, the team's knowledge of the system, and their own experience and judgment. However, estimates within an order of magnitude are sufficiently accurate for the purpose of risk analysis in most cases. Later, at the time of selecting safeguards, if it becomes important to refine specific items, that can be done, but during the analysis gross statements of impact and frequency are all that are required.

4.2 Expressions of Impact and Frequency

Quantitative means of expressing both potential impact and estimated frequency of occurrence are necessary to performing a risk analysis.

To date no better common denominator has been found for quantifying the impact of an adverse circumstance—whether the damage is actual or abstract, the victim a person, a piece of equipment or a function—than monetary value. It is the recompense used by the courts to redress both physical damage and mental anguish. Some methodologies advocate the use of abstract symbols of impact. "$" is, in fact, a symbol, yet one which transfers directly to fiscal usage without any intermediate translation.

Since impact will be expressed monetarily and fiscal matters are organized on an annual basis in Federal agencies, a year is the most suitable time period to specify in expressing expected frequency of occurrence of threats. Some threats occur only once in a number of years while others happen many times a day. Such frequencies are not always easy to express in terms of years: "five times a day," for instance, converts to "1825 times a year" and "once every five years" converts to "one-fifth of an occurrence per year."

The time needed for the analysis will be considerably reduced, and its usefulness will not be decreased, if both impact and frequency estimates are rounded to the factors of ten shown in figure 1. There will be no significant difference in the overall exposure whether the damage from a certain event is estimated at $110,000 or $145,000. Assigning value to such things as loss of career caused by disclosure of confidential data or suffering caused by undue delay in the delivery of an annuity check is, in fact, more readily done in orders of magnitude than in actual figures. Here again, there will be no difference if the frequency of an event is expected to be twelve times a year or thirty. Using the scales for frequency from figure 1 will avoid the use of unwieldy fractions and maintain the flexibility to work with high probability events in days and low probability events in years.

IMPACT:
$10
$100
$1000
$10,000
$100,000
$1,000,000
$10,000,000
$100,000,000

FREQUENCY:
Once in 300 years
Once in 30 years
Once in 3 years (1000 days)
Once in 100 days
Once in 10 days
Once per day
10 times per day
100 times per day

FIGURE 1. *Orders of Magnitude of Estimated Impact and Frequency.*

4.3 Annual Loss Exposure

If the impact of an event, i.e., the precise amount of damage it could cause, and the frequency of occurrence of that event, i.e., the exact number of times it could happen, could be specified, the product of the two would be a statement of loss, or

$$\text{Loss} = \text{Impact} \times \text{Frequency of Occurrence.}$$

However, because the exact impact and frequency can usually not be specified, it is only possible to approximate the loss with an annual loss exposure (ALE), which is the product of estimated impact in dollars (I) and estimated frequency of occurrence per year (F).

For ease in use, the orders of magnitude for estimated impact and estimated frequency of occurrence can be indexed, as shown in figure 2.

When i and f are indices to possible orders of impact and frequency,

the relationship of i to I is $I = 10^i$ and

the relationship of f to F is $F = \frac{10^{(f-3)}}{3}$

or $$F = \frac{10^f}{3000}.$$

Thus the annual loss expectancy can be calculated by the formula

$$ALE = \frac{10^i}{3} \times 10^{(f-3)},$$

which reduces to

$$ALE = \frac{10^{(f+i-3)}}{3}.$$

Using the table shown in figure 3 will be faster than following the formula for ALE but will produce the same result. Find the appropriate row and column for the i and f selected from figure 2; the cell where they intersect will contain the ALE.

If the estimated cost impact of the event is

$10, let i = 1
$100, let i = 2
$1000, let i = 3
$10,000, let i = 4
$100,000, let i = 5
$1,000,000, let i = 6
$10,000,000, let i = 7
$100,000,000, let i = 8

If the estimated frequency of occurrence is

Once in 300 years, let f = 1
Once in 30 years, let f = 2
Once in 3 years, let f = 3
Once in 100 days, let f = 4
Once in 10 days, let f = 5
Once per day, let f = 6
10 times per day, let f = 7
100 times per day, let f = 8

FIGURE 2. *Tables for Selecting of Values of i and f.*

Values of F

Values of i	1	2	3	4	5	6	7	8
1					$300	$ 3k	$ 30k	$300k
2				$300	3k	30k	300k	3M
3			$300	3k	30k	300k	3M	30M
4		$300	3k	30k	300k	3M	30M	300M
5	$300	3k	30k	300k	3M	30M	300M	
6	3k	30k	300k	3M	30M	300M		
7	30k	300k	3M	30M	300M			

Values of ALE

FIGURE 3. *Table for Determining Values of ALE.*

The tables from figures 2 and 3 can be combined as shown in figure 4 for greater convenience.

		Once in 300 yrs (100,000 days)	Once in 30 yrs (10,000 days)	Once in 3yrs (1,000 days)	Once in 100 days	Once in 10 days	Once per day	10 per day	100 per day
	f= / i=	1	2	3	4	5	6	7	8
$10	1					$300	$3,000		$300k
$100	2				$300	$3,000	$30k	$300k	$3M
$1000	3			$300	$3,000	$30k	$300k	$3M	$30M
$10,000	4		$300	$3,000	$30k	$300k	$3M	$30M	
$100,000	5	$300	$3,000	$30k	$300k	$3M	$30M	$300M	
$1,000,000	6	$3,000	$30k	$300k	$3M	$30M	$300M		
$10,000,000	7	$30k	$300k	$3M	$30M	$300M			
$100,000,000	8	$300k	$3M	$30M	$300M				

FIGURE 4. *Combined Matrix of i, f and ALE.*

4.4 Procedure

The team will need an organized way of approaching their task and an orderly method of recording their findings. It would probably be impossible for the team to conceive of every event which could have a deleterious effect on data processing. Therefore, the risk analysis task is better approached from the standpoint of the data files, or applications systems, of which there is a finite number. Cataloging each data file or application system on a worksheet on which the results of the analysis can also be noted will give structure to the task.

Worksheets may be formatted in any way an agency finds useful, but they should be as simple as possible and should not contain any superfluous data. The worksheet shown in figure 5 can be copied and enlarged to provide more working space, if desired.

All of the organization's application systems, or data files arranged by application, should be listed on the worksheet(s). By tracing the flow of data through a system, the team will be able to pinpoint where in the processing the threats identified in the preliminary study could occur. Because of the preliminary vulnerability study and the team's collective familiarity with the systems/applications/files, they should be able to assign reasonable estimated frequencies to such events. If a file is used with more than one application system, it should be listed under each, as it can be vulnerable to different hazards under different systems.

Organizations with a large number of files will probably want in their initial risk analysis to consider their data on an application basis rather than on a file basis because of the size of the task awaiting them. Such an analysis should be followed by the more detailed file-by-file consideration in any instances where there is an indication that protection requirements differ radically among the files in any one application system.

The values of i and f should be filled in at each intersection on the worksheet, as should the value of ALE, or it will be impossible to reconstruct the basis for a particular ALE. Keep a running total of the ALEs attributable to each threat on the list of actual threats. (If additional threats surface, they should be added to the list.) A note in the "Comments" column linking the ALE to the particular threat, or threats, will be useful at the time of selecting remedial measures.

The effect of currently installed protective measures on undesirable events should not be taken into account at this stage. Their consideration would require efficacy judgments which are properly a part of the subsequent safeguard selection process.

Where more than one circumstance can affect data integrity, data confidentiality or processing availability, the i and f values for these events should be noted separately; this will be an aid in deciding on security measures. Use the "Comments" column to note the steps or functions in a system where problems can occur. When the team is considering data confidentiality, their task can be simplified by first eliminating the files which are known to contain no personal, proprietary or other information of a nature which would make disclosure a problem.

The further division of data integrity into modification and destruction is necessary because the two will not always have the same impact, nor occur with the same frequency.

The "Comments" column can be used as shown in figures 6 and 7 to indicate the processing step in which a destructive event can occur. It can also be used to refer to additional notes which may be needed to explain certain situations more completely.

The time periods in the "Processing Availability" column are mission dependent and will have to be determined by each organization for itself. They will be important in the selection of backup facilities and should be subject to review by top management. The destruction of equipment should be considered under "Processing Availability" because the ultimate effect of destroying equipment will be the inability to process data. The impact will be the cost associated with the inability to process rather than the cost of replacing equipment. Replacement is a possible remedial measure, the cost of which should be subjected to the same analysis as any other measure (as described in Chapter 6).

4.5 Special Advice

ADP risk analysis is a technique which relies heavily on the intuition, experience and technical knowledge of the team members. The

SYSTEM/APPLICATION Data Files	DATA INTEGRITY		DATA CONFIDENTIALITY	PROCESSING AVAILABILITY			COMMENTS
	Modification	Destruction					
	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	

FIGURE 5. *Risk Analysis Worksheet.*

comments in this section are included for the purpose of putting certain problems in perspective and giving the team confidence in its own collective judgment in areas where there often appears to be little or no precedent or guidance on which to base a decision.

4.5.1 Human Frailty

The team will come upon doubts as they weigh the part personal integrity plays in the security of a system. While every Federal employee who works in an ADP environment must have a clearance appropriate to the content or purpose of the systems he deals with, there is no way of knowing at any time what stresses are operating on an individual—what pressures he has at home, what jealousies exist in the work situation, what financial burdens he is under. For these reasons, it is usually best to leave individual personal integrity out as a factor contributing to security in a risk analysis. The right time for considering personal integrity is during development of the security plan, when various safeguards can be discussed.

Several general conclusions seem to be emerging from the growing body of statistics on computer crime [10]:

- The vast majority of white collar crime is committed by employees defrauding their own employers.
- In general, employees who defraud their employers do so using resources to which they have access in the course of their jobs.
- The best deterrent to white collar crime has proved to be curtailment of incentive, i.e., limiting the profit potential of dishonest activity to the minimum consistent with the assigned task. If employees can expect no more than minimal gain from unscrupulous acts, they will be less likely to attempt them. The second-best deterrent is the fear of getting caught. If employees know there is adequate surveillance of activity, they will be less apt to place themselves in jeopardy.

4.5.2 Physical Security/Inability to Process

Another difficulty the team can encounter is the confusion caused by treating fires, floods and other natural disasters solely as physical security problems. While the initial impact of natural disasters usually is physical destruction, there can be other less immediately obvious effects on processing capability, such as loss of utilities, loss of the services of key personnel and damage to data storage media. There can also be loss of services without any damage to a facility.

The loss of the physical facility and the loss of processing availability should be treated independently of each other, since neither necessarily causes the other. The total inability to process can be caused by circumstances other than physical destruction. For instance, hardware malfunctions can hold up all processing for several days; accidental erasure of critical programs or data can delay an urgent task for many hours; a fire in another building can deprive the ADP center of utilities; waterlogging of preprinted output forms can halt output until the forms can be replaced, possibly a matter of weeks. Flood damage can result not only from overflowing rivers, but also from leaky fixtures, bursting pipes or fire fighting activity nearby.

4.5.3. Estimating Frequency of Occurrence

At first the team may feel that estimating frequency of events for which there is no history of occurrence is impossible. Common sense, however, can help. Consider, for example, a payment system with good automated controls over the number of checks and the sums of the amounts of the checks. Between a hundred and a thousand people may know that it is relatively easy to change a recipient's address without risk that it will be detected; one of them could easily divert checks to an address where they could be picked up and cashed by someone other than the intended recipient. Such a situation should yield an estimated frequency much higher than once in thirty years and probably much lower than once every ten days, leaving the choice between once every three years and once every hundred days. Selecting the most appropriate of these figures depends on several factors, including the general atmosphere in which the system functions. If the number of people who know of the vulnerability is one or two hundred, the former is the most likely figure. If the number of people who know is nearer a thousand, or if employee dishonesty is accepted by management as long as it stays within established bounds,

then the higher estimated frequency would be more likely.

4.6 Sensitivity of Documentation

All reports, worksheets and any other documentation or notes dealing with the risk analysis should be treated as highly sensitive and should be so marked by whatever method the organization uses.

5. AN EXAMPLE

An example using a hypothetical government agency has been developed to show some of the facets which must be considered in a risk analysis. Only a small part of the agency's total ADP applications are considered here.

5.1. General Environment

5.1.1. Central Computer Facility

- The central ADP facility is housed in a separate three-story wing of the agency's headquarters in central Kansas.
- The equipment consists of a large-scale processor with 3 CPUs, 32 tape drives, 10 billion characters of disk storage, 3 front-end communications processors capable of handling a total of 175 terminals (125 are presently in the system), a COM unit and a library of 50,000 reels of tape. Transmission between central facility and terminals is by private leased line.
- Guards check all personnel into and out of the computer area. Badges are required. Areas not monitored by guards are controlled by an electronic card system. Procedures are in effect covering lost, forgotten, stolen and damaged badges and card passes and the issuance of badges to visitors.
- There is a supervised fire detection/suppression system consisting of products-of-combustion detectors and a dry-pipe sprinkler system. Hand extinguishers are located throughout the facility, the type determined by the equipment or supplies in their vicinity. Continuing emergency team training is required of all computer operations personnel. The training includes actual use of the various extinguishers. Fire safety orientation is given to all employees when first hired and annually thereafter. Areas of the building adjacent to the computer facility do not have fire detection devices. These areas are under the control of operating units other than data processing.
- There is no emergency power or uninterruptible power supply backup. In the last seven years, the facility has experienced machine failure due to power outages resulting from thunderstorms, a fire at the utility substation and breaks in the main power feeder caused by a construction project. In recent months (especially summer) local brownouts have caused the failure of certain electronic equipment. These brownouts occur about every three weeks.
- The air conditioning unit is five years old and has suffered three breakdowns: one 2 years after installation, one 18 months later, and a third after another year. Two 100-ton cooling towers are located on the roof of the wing in which the ADP facility is located.
- Plastic covers are supplied for all hardware in the facility. The flooring is raised 24 inches and there are automatic pumps in case of water entry. The tape library is well protected from water damage.
- Emergency power-down switches are provided for all computer and air conditioning systems.
- Management is aware that, annually, about 400 tape and/or disk files are misplaced or destroyed by improper handling or overwriting because of incorrect labeling.
- Employee morale is notably high. The agency has established good personnel policies and the procedures for dealing with

employee complaints work fairly and to the satisfaction of most. All ADP personnel are aware of management's continuing interest in maintaining and enforcing security procedures at both central and remote facilities.

- The operating system must be restarted several times a week. Sometimes the problem can be traced to a hardware failure, but usually it is not resolved. Systems programmers maintain the system with little direct supervision. There is no formal review before changes are installed. The operators have learned how to keep the system running efficiently, but some of the evening and night supervisors have little understanding of what the operators do.

5.1.2 Terminals

- The remote job entry terminals are all located in GSA leased spaces, one at each field office. They are locked when unattended; however, they are used by several branches of the agency for a number of systems. Magnetic tapes are secured in locked cabinets located in terminal rooms. Data tapes are retained for one month only. Source documents on microfilm are stored in secure areas other than in the terminal room. Data are not protected during transmission from terminals to central facility.

5.1.3 Backup Facilities

- No plans have been made for emergency backup of automatic data processing.

5.2 Specific Systems

5.2.1 Application 100

This application supports a mission stemming from an Executive Order requiring a report to be produced and published on the third Thursday of each month. It has been automated for ten years. A master file containing the most recent report must be updated monthly with new data transmitted from 30 field offices to the central facility. When the new data are merged, a new report is produced and distributed through controlled official channels.

The following set of circumstances is assumed for this application:

- The data are necessary to the Federal community. Their output can have an economic impact on the private sector if released early.
- At the field offices, the source documents are microfilmed after data have been translated into machine readable format (magnetic tape). Seven of the offices have their own microfilming equipment; twenty-three have it done on contract.
- Data transmission to central facility is accomplished during third shift operation (0001 to 0800) every Tuesday.
- If communications network is down, data tapes are flown to the central facility. Communications failure occurs an average of three times a year.
- Only ADP personnel with appropriate clearances are authorized to handle the data throughout the entire process.
- To date, there have been no known incidents of unauthorized access to or early release of the data.
- Copies of updated reports are stored at the central facility in a special locked cabinet and backup copies are stored at a GSA Records Center. The backup copies are maintained for three (3) cycles—current, plus two most recent months.
- A part of the final report, Section A, is created from some preliminary data. It must be available two days before the final data are transmitted so that analysis can be started. Updating the previous month's report requires preparation of the master tape. Certain other tape files must be used in this process; these include personnel assignment data, regional projects data and budget status data.
- Each of the elements is considered critical to the final product. At the conclusion of each stage, checks are made for errors which might have been introduced. No major errors have ever been detected. Errors which have been found are restricted primarily to the new data tapes created by field offices.
- If the system were to be violated, or if the report were to be late, some adverse impact would be felt in the stock markets. There would be embarrassment to the Govern-

ment on both national and international scenes.

- The data are of such importance to "outside" individuals that relatively senior personnel could be tempted to obtain prerelease information or cause the final report to miss the established publication date.
- All personnel involved are continuously observed by their managers for any signs of attitude change, deterioration in performance, or other indications of situations that could result in breaches to the security of this project.
- All corrections, updates, or modifications to the software systems are closely monitored and tested before final approval and subsequent incorporation into the master system.

The system consists of the six stages shown below:

INPUT	PROCESS	OUTPUT
Stage 1—Data preparation		
Source data	key to tape verify duplicate microfilm destroy source documents	Source data tape + 1 copy microfilm
Stage 2—Data transmission		
Source data tape	transmit verify	Change data tape
Stage 3—File maintenance		
Master tape (current) Change data tape	update verify duplicate tape	Master tape (new + 1 cy)
Stage 4—Section A creation		
Master tape Personnel assignment data Regional project data Budget status data	calculate format	Sect A report
Stage 5—Final report creation		
Master tape Personnel assignment data Regional projects data Budget status data	same as St. 4	Final report
Stage 6—Querying		
Master tape Personnel assignment data Regional projects data	search read	video display

The worksheet for this application is shown in figure 6.

SYSTEM/APPLICATION Data Files	DATA INTEGRITY				DATA CONFIDENTIALITY		PROCESSING AVAILABILITY			COMMENTS
	Modification		Destruction				2 hrs	24 hrs	72 hrs	
APPLICATION 100	(i) (ALE)	(f)	(i) (ALE)	(f)	(i) (ALE)	(f)	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	
Source Documents	4	1	4	1	5 $3k	2[a]	–	–	–	a. key to tape, st. 1, Thr. 9
Source data tape	4 $30k	4[a]	3	2	5 $30k	3[a]	–	–	–	a. key to tape, st. 1, Thr. 9
Microfilm	–		–		5 $30k	3[a]	–	–	–	a. microfilm, st. 1 Thr. 9
Change data tape	3 $300	3[a]	3 $300	3[a]	5 $300k	4[a]	–	6 3[a] $300k	–	a. transmit, st. 2, Thr. 21
Master tape	5 $30k	3	5 $30k	3[a,b]	7 $30M	4[a,b,c]	7 4[a,b,d] $30M	–	–	a. entire operation, st. 4, Thr. 14 b. entire operation, st. 5, Thr. 14 c. read, st. 6, Thr. 14 d. power interrupt, op. shut down
Personnel assignment data	5 $300	1	5 $300	1	5 $300	1	5 3[a] $30k	–	–	a. calculate, st. 4, 5, Thr. 19, 23
Regional projects data	3 $300	2[a]	3	1	4 $300	2[a]	5 3[a] $30k	–	–	a. calculate, st. 4, 5, Thr. 19, 23
Budget status data	3	1	3	1	4	1	5 3[a] $30k	–	–	a. calculate, st. 4, 5, Thr. 19, 23

FIGURE 6. *Risk Analysis Worksheet for Application 100.*

5.2.2 Application 870

This system is used to maintain and control the agency's plans and gross budgetary information for the most recent five years, the current year and the next five: ProgHist, CurrProg and AgPlans. The software consists of an agency developed program, PFiles, and a commercial proprietary program, WWWMod, which does the modeling required to choose the optimum course for future plans.

There are six video graphics terminals equipped with hard copy printers located in the offices of top management and a small control center with a large video screen in the office of the head of the agency to be used for displaying the results of on-line modeling at staff meetings. All files are mounted on-line during normal working hours. They are updated after every working day at 1:00 a.m. with the previous day's transactions—an average of ten, except during February and August when processing time jumps from 1.8 hours a month to 4 hours a month.

The system consists of the three stages shown below:

INPUT	PROCESS	OUTPUT
Stage 1—Daily file maintenance	(1 am, 1.8 hrs/mo, except Feb and Aug 4 hrs/mo)	
CurrProg	update files	CurrProg
PFiles	verify	
	duplicate	
Stage 2—Querying & modeling	(8 am to 5 pm daily)	
AgPlans	search files	video display
CurrProg	read files	printout
WWWMod	calculate	
Stage 3—Semiannual report creation	(during working hours, Feb and Aug)	
AgPlans	calculate	MBOfuture rpt
CurrProg	verify	(2cc only)
ProgHist	format	AgPlans
WWWMod	update AgPlans	ProgHist
PFiles	update ProgHist	video display
	verify	

The worksheet for this application is shown in figure 7.

SYSTEM/APPLICATION Data Files	DATA INTEGRITY		DATA CONFIDENTIALITY	PROCESSING AVAILABILITY			COMMENTS
	Modification	Destruction		2 hrs	24 hrs	72 hrs	
APPLICATION 870	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	
AgPlans	6 3 $300k	4 2 $300	7 4 $30M	–	–	–	
CurrProg	5 3 $30k	4 2 $300	6 3 $300k	–	–	–	
ProgHist	4 2 $300	–	–	–	–	–	
WWWMod	4 3 $3k	4 2 $300	4 3 $3k	–	–	–	
PFiles	4 2 $300	4 2 $300	4 2 $300	–	–	–	

FIGURE 7. *Risk Analysis Worksheet for Application 870.*

6. SELECTION OF SAFEGUARDS

6.1 Alternative Measures

In the process of deciding which protective measures will provide the best overall security, management should look first to procedural and physical safeguards. Procedural controls, especially when used in combination with physical barriers, produce the highest degree of security for the lowest cost of all forms of protection. They satisfy the requirements of the Privacy Act of 1974 as well as many other demands either dictated by prudence or mandated by regulations. Procedural measures range from screening of all applicants before employment to off-site storage of backup data to standards for program development to preparation and testing of contingency plans. Procedural measures are essential for filling the gaps between manual and automated processing, between human beings and systems hardware and software. They are very effective against accidents resulting from human negligence and against amateur thievery. They promote an atmosphere of managerial concern for data and processing security that tends to discourage all but the most determined felons.

Most measures are effective against more than one threat. Maintaining facility access logs is a method of controlling who goes into a facility, of knowing who is in a facility at a given time, and of preventing unauthorized removal of material from a facility. Encryption protects data both during transmission and while in storage. Audit trails furnish information for backup and recovery and also provide a basis for variance detection.

Returning to the examples in section 5: it was found in Application 870 that though the files were very seldom used, they were on line throughout working hours, which greatly increased their vulnerability. The protection needs could be greatly reduced if the files were only available to an application running on a dedicated processor. This could be handled on a scheduled basis or on a given amount of notice. A several million dollar exposure could be circumvented in this way for only the cost of reviewing the system requirements. In Application 100 the losses that could occur at the field offices were found to be minor and appeared upon examination to be of a nature which could be averted by implementing procedural measures. The largest losses that could occur in the system were related directly to the data on the master tape and to the availability of processing to convert the data on the master tape into the required report. It was obvious that safeguards for protecting these two areas would also have an advantageous effect on many of the smaller concerns that were noted.

System security measures should be contemplated only after it has been established that physical and procedural safeguards are insufficient to meet the organization's protective requirements. If an organization's needs dictate the use of software or hardware protection for some systems, then those measures can also be incorporated in the protection plan for systems with lesser requirements, provided the operating costs of those systems are not thereby inordinately increased.

6.2 ALE Reduction vs Cost

The cost of each measure should be considered in three different ways: first, vis-à-vis the ALE reduction it brings about, then the total cost of the combined measures should be considered in relation to the net ALE reduction, and finally the additional ALE reduction by each measure should be compared to its share of the total cost. The selection of security measures is also discussed in FIPS PUB 31[6], FIPS PUB 41[1] and NBS Special Publication 500-33[2].

By constructing a matrix such as shown in figure 8, the threats and the protective measures which could affect one or more of them can be displayed. The threats should be arranged in order of ALEs attributable to them (highest to lowest). Each intersection in the matrix should contain three pieces of information: (a) the estimated ALE reduction, (b) the annual cost of the measure, and (c) the resultant annual saving. Great precision is not necessary in arriving at these three figures. The annual cost of a measure is listed opposite the most serious threat which it affects; opposite any other threat which is affected only the increase in cost to cover that threat is noted.

THREATS	MEASURES	A	B	C	D
1	(a)	*$20,000	$20,000	$18,000	
	(b)	9,000	15,000	8,000	
	(c)	11,000	5,000	10,000	
2	(a)	10,000	12,000	—	
	(b)	—	—		
	(c)	10,000	12,000		
3	(a)	4,000	6,000	—	
	(b)	1,000	—		
	(c)	3,000	6,000		
4	(a)	2,000	4,000	—	
	(b)	5,000	2,000		
	(c)	−3,000	2,000		

*See paragraph above.

FIGURE 8. *Array of Remedial Measures vs Threats.*

Now is the correct time to evaluate the usefulness of existing security measures to the overall security of the facility. They should all be included in the matrix but only the annual maintenance costs need be considered, not the initial installation costs since those have already been expended. The cost of those which are not solely for the purpose of computer security should be prorated if possible. It is also the correct time to consider replacement costs. Replacement of equipment should be treated the same as any other remedial measure. It may develop that the cost of replacing equipment is less, in some cases, than protecting it.

Comparing all the measures which remedy the same threat (or lesser included threats) will show which one is the most cost effective in the given circumstances. In the matrix above, protective measure A, costing $10,000, provides a $24,000 saving against threats 1, 2 and 3 while measure B, costing $17,000, provides a $25,000 summed saving against threats 1, 2, 3 and 4. The two measures together, at a cost of $27,000, provide an ALE reduction of $31,000. However, the final comparison reveals that the $10,000 expenditure for measure A only produces an additional saving of $6,000 over that obtained by the $17,000 expenditure. In some circumstances it may be determined that the additional reduction is necessary; in other less sensitive situations, the cost saving will be adopted instead. In addition, care should be taken to insure that the measures chosen to counter certain threats do not increase the estimated frequency of other threats.

With all of the ALE reduction and cost figures arrayed, various combinations of safeguards can be considered tentatively until a satisfactory aggregation of security measures is achieved. The matrix will be useful in explaining to management why particular safeguards should be selected.

The matrix and all other material associated with the risk analysis should be treated as highly sensitive. Copies of all letters, papers, worksheets and reports prepared by the risk analysis team should be preserved for the information of those performing subsequent risk analyses.

APPENDIX

A. APPLICATION SYSTEM VULNERABILITIES

It will be useful to the team, as they consider applications systems and data files, to be aware of the many undesirable events which can have serious consequences. A number of situations to which applications systems are vulnerable are listed here, grouped according to common system organizational structures. The list is not intended to be all-inclusive but only to

suggest the various kinds of vulnerabilities that may exist in each system.

1. ERRONEOUS OR FALSIFIED DATA INPUT. Erroneous or falsified input data is the simplest and most common cause of undesirable performance by an applications system. Vulnerabilities occur wherever data is collected, manually processed, or prepared for entry to the computer.

- Unreasonable or inconsistent source data values may not be detected.
- Keying errors during transcription may not be detected.
- Incomplete or poorly formatted data records may be accepted and treated as if they were complete records.
- Records in one format may be interpreted according to a different format.
- An employee may fraudulently add, delete, or modify data (e.g., payment vouchers, claims) to obtain benefits (e.g., checks, negotiable coupons) for himself.
- Lack of document counts and other controls over source data or input transactions may allow some of the data or transactions to be lost without detection—or allow extra records to be added.
- Records about the data-entry personnel (e.g., a record of a personnel action) may be modified during data entry.
- Data which arrives at the last minute (or under some other special or emergency condition) may not be verified prior to processing.
- Records in which errors have been detected may be corrected without verification of the full record.

2. MISUSE BY AUTHORIZED END USERS. End users are the people who are served by the ADP system. The system is designed for their use, but they can also misuse it for undesirable purposes. It is often very difficult to determine whether their use of the system is in accordance with the legitimate performance of their job.

- An employee may convert Government information to an unauthorized use; for example, he may sell privileged data about an individual to a prospective employer, credit agency, insurance company, or competitor; or he may use Government statistics for stock market transactions before their public release.
- A user whose job requires access to individual records in a file may manage to compile a complete listing of the file and then make unauthorized use of it (e.g., sell a listing of employees' home addresses as a mailing list).
- Unauthorized altering of information may be accomplished for an unauthorized end user (e.g., altering of personnel records).
- An authorized user may use the system for personal benefit (e.g., theft of services).
- A supervisor may manage to approve and enter a fraudulent transaction.
- A disgruntled or terminated employee may destroy or modify records—possibly in such a way that backup records are also corrupted and useless.
- An authorized user may accept a bribe to modify or obtain information.

3. UNCONTROLLED SYSTEM ACCESS. Organizations expose themselves to unnecessary risk if they fail to establish controls over who can enter the ADP area, who can use the ADP system, and who can access the information contained in the system.

- Data or programs may be stolen from the computer room or other storage areas.
- ADP facilities may be destroyed or damaged by either intruders or employees.
- Individuals may not be adequately identified before they are allowed to enter ADP area.
- Remote terminals may not be adequately protected from use by unauthorized persons.
- An unauthorized user may gain access to the system via a dial-in line and an authorized user's password.
- Passwords may be inadvertently revealed to unauthorized individuals. A user may write his password in some convenient place, or the password may be obtained from card decks, discarded printouts, or by observing the user as he types it.
- A user may leave a logged-in terminal unattended, allowing an unauthorized person to use it.
- A terminated employee may retain access to ADP system because his name and pass-

word are not immediately deleted from authorization tables and control lists.

- An unauthorized individual may gain access to the system for his own purposes (e.g., theft of computer services or data or programs, modification of data, alteration of programs, sabotage, denial of services).
- Repeated attempts by the same user or terminal to gain unauthorized access to the system or to a file may go undetected.

4. INEFFECTIVE SECURITY PRACTICES FOR THE APPLICATION. Inadequate manual checks and controls to insure correct processing by the ADP system or negligence by those responsible for carrying out these checks result in many vulnerabilities.

- Poorly defined criteria for authorized access may result in employees not knowing what information they, or others, are permitted to access.
- The person responsible for security may fail to restrict user access to only those processes and data which are needed to accomplish assigned tasks.
- Large funds disbursements, unusual price changes, and unanticipated inventory usage may not be reviewed for correctness.
- Repeated payments to the same party may go unnoticed because there is no review.
- Sensitive data may be carelessly handled by the application staff, by the mail service, or by other personnel within the organization.
- Post-processing reports analyzing system operations may not be reviewed to detect security violations.
- Inadvertent modification or destruction of files may occur when trainees are allowed to work on live data.
- Appropriate action may not be pursued when a security variance is reported to the system security officer or to the perpetrating individual's supervisor; in fact, procedures covering such occurrences may not exist.

5. PROCEDURAL ERRORS WITHIN THE ADP FACILITY. Both errors and intentional acts committed by the ADP operations staff may result in improper operational procedures, lapsed controls, and losses in storage media and output.

Procedures and Controls:

- Files may be destroyed during data base reorganization or during release of disk space.
- Operators may ignore operational procedures; for example, by allowing programmers to operate computer equipment.
- Job control language parameters may be erroneous.
- An installation manager may circumvent operational controls to obtain information.
- Careless or incorrect restarting after shutdown may cause the state of a transaction update to be unknown.
- An operator may enter erroneous information at CPU console (e.g., control switch in wrong position, terminal user allowed full system access, operator cancels wrong job from queue).
- Hardware maintenance may be performed while production data is on-line and the equipment undergoing maintenance is not isolated.
- An operator may perform unauthorized acts for personal gain (e.g., make extra copies of competitive bidding reports, print copies of unemployment checks, delete a record from journal file).
- Operations staff may sabotage the computer (e.g., drop pieces of metal into a terminal).
- The wrong version of a program may be executed.
- A program may be executed using wrong data or may be executed twice using the same transactions.
- An operator may bypass required safety controls (e.g., write rings for tape reels).
- Supervision of operations personnel may not be adequate during non-working hour shifts.
- Due to incorrectly learned procedures, an operator may alter or erase the master files.
- A console operator may override a label check without recording the action in the security log.

Storage Media Handling:

- Critical tape files may be mounted without being write protected.

- Inadvertently or intentionally mislabeled storage media are erased. In a case where they contain backup files, the erasure may not be noticed until it is needed.
- Internal labels on storage media may not be checked for correctness.
- Files with missing or mislabeled expiration dates may be erased.
- Incorrect processing of data or erroneous updating of files may occur when card decks have been dropped, partial input decks are used, write rings mistakenly are placed in tapes, paper tape is incorrectly mounted, or wrong tape is mounted.
- Scratch tapes used for jobs processing sensitive data may not be adequately erased after use.
- Temporary files written during a job step for use in subsequent steps may be erroneously released or modified through inadequate protection of the files or because of an abnormal termination.
- Storage media containing sensitive information may not get adequate protection because operations staff is not advised of the nature of the information content.
- Tape management procedures may not adequately account for the current status of all tapes.
- Magnetic storage media that have contained very sensitive information may not be degaussed before being released.
- Output may be sent to the wrong individual or terminal.
- Improperly operating output or post-processing units (e.g., bursters, decollators or multipart forms) may result in loss of output.
- Surplus output material (e.g., duplicates of output data, used carbon paper) may not be disposed of properly.
- Tapes and programs that label output for distribution may be erroneous or not protected from tampering.

6. PROGRAM ERRORS. Applications programs should be developed in an environment that requires and supports complete, correct, and consistent program design, good programming practices, adequate testing, review, and documentation, and proper maintenance procedures. Although programs developed in such an environment will still contain undetected errors, programs not developed in this manner will probably be rife with errors. Additionally, programmers can deliberately modify programs to produce undesirable side effects or they can misuse the programs they are in charge of.

- Records may be deleted from sensitive files without a guarantee that the deleted records can be reconstructed.
- Programmers may insert special provisions in programs that manipulate data concerning themselves (e.g., payroll programmer may alter his own payroll records).
- Data may not be stored separately from code with the result that program modifications are more difficult and must be made more frequently.
- Program changes may not be tested adequately before being used in a production run.
- Changes to a program may result in new errors because of unanticipated interactions between program modules.
- Program acceptance tests may fail to detect errors that only occur for unusual combinations of input (e.g., a program that is supposed to reject all except a specified range of values actually accepts an additional value).
- Programs, the contents of which should be safeguarded, may not be identified and protected.
- Code, test data with its associated output, and documentation for certified programs may not be filed and retained for reference.
- Documentation for vital programs may not be safeguarded.
- Programmers may fail to keep a change log, to maintain back copies, or to formalize recordkeeping activities.
- An employee may steal programs he is maintaining and use them for personal gain (e.g., sale to a commercial organization, hold another organization for extortion).
- Poor program design may result in a critical data value being initialized twice. An error may occur when the program is modified to change the data value—but only changes it in one place.
- Production data may be disclosed or

destroyed when it is used during testing.
- Errors may result when the programmer misunderstands requests for changes to the program.
- Errors may be introduced by a programmer who makes changes directly to machine code.
- Programs may contain routines not compatible with their intended purpose, which can disable or bypass security protection mechanisms. For example, a programmer who anticipates being fired inserts code into a program which will cause vital system files to be deleted as soon as his name no longer appears in the payroll file.
- Inadequate documentation or labeling may result in wrong version of program being modified.

7. OPERATING SYSTEM FLAWS. Design and implementation errors, system generation and maintenance problems, and deliberate penetrations resulting in modifications to the operating system can produce undesirable effects in the application system. Flaws in the operating system are often difficult to prevent and detect.
- User jobs may be permitted to read or write outside assigned storage area.
- Inconsistencies may be introduced into data because of simultaneous processing of the same file by two jobs.
- An operating system design or implementation error may allow a user to disable audit controls or to access all system information.
- The operating system may not protect a copy of information as thoroughly as it protects the original.
- Unauthorized modification to the operating system may allow a data entry clerk to enter programs and thus subvert the system.
- An operating system crash may expose valuable information such as password lists or authorization tables.
- Maintenance personnel may bypass security controls while performing maintenance work. At such times the system is vulnerable to errors or intentional acts of the maintenance personnel, or anyone else who might also be on the system and discover the opening (e.g., microcoded sections of the operating system may be tampered with or sensitive information from on-line files may be disclosed).
- An operating system may fail to record that multiple copies of output have been made from spooled storage devices.
- An operating system may fail to maintain an unbroken audit trail.
- When restarting after a system crash, the operating system may fail to ascertain that all terminal locations which were previously occupied are still occupied by the same individuals.
- A user may be able to get into monitor or supervisory mode.
- The operating system may fail to erase all scratch space assigned to a job after the normal or abnormal termination of the job.
- Files may be allowed to be read or written without having been opened.

8. COMMUNICATIONS SYSTEM FAILURE. Information being routed from one location to another over communication lines is vulnerable to accidental failures and to intentional interception and modification by unauthorized parties.

Accidental Failures:
- Undetected communications errors may result in incorrect or modified data.
- Information may be accidentally misdirected to the wrong terminal.
- Communication nodes may leave unprotected fragments of messages in memory during unanticipated interruptions in processing.
- Communication protocol may fail to positively identify the transmitter or receiver of a message.

Intentional Acts:
- Communications lines may be monitored by unauthorized individuals.
- Data or programs may be stolen via telephone circuits from a remote job entry terminal.
- Programs in the network switching computers may be modified to compromise security.
- Data may be deliberately changed by individuals tapping the line (requires some

sophistication, but is applicable to financial data).

- An unauthorized user may "take over" a computer communication port as an authorized user disconnects from it. Many systems cannot detect the change. This is particularly true in much of the currently available communication equipment and in many communication protocols.
- If encryption is used, keys may be stolen.
- A terminal user may be "spoofed" into providing sensitive data.
- False messages may be inserted into the system.
- True messages may be deleted from the system.
- Messages may be recorded and replayed into the system ("Deposit $100" messages).

REFERENCES AND SUGGESTED READING

1. Computer Security Guidelines for Implementing the Privacy Act of 1974, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication (FIPS PUB) 41, National Technical Information Service, Springfield, VA (1975).
2. Courtney, Robert H., Jr. and Orceyre, Michael J., Considerations in the Selection of Security Measures. National Bureau of Standards (U.S.) Special Publication 500-33, Government Printing Office, Washington, DC (1978).
3. Data Security Controls and Procedures—A Philosophy for DP Installations, G320-5649-00, IBM Corporation, White Plains, NY (1976).
4. Disaster Preparedness, Office of Emergency Preparedness Report to Congress, Stock Number 4102-0006, Government Printing Office, Washington, DC (1972).
5. Glossary for Computer Systems Security, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication (FIPS PUB) 39, National Technical Information Service, Springfield, VA (1976).
6. Guidelines for ADP Physical Security and Risk Management, National Bureau of Standards (U.S.), Federal Information Processing Standards Publication (FIPS PUB) 31, National Technical Information Service, Springfield, VA (1974).
7. Hoyt, Douglas B., Ed., Computer Security Handbook, McMillan Information, New York (1973).
8. Martin, James, Security, Accuracy and Privacy in Computer Systems, Prentice-Hall, Inc., Englewood Cliffs, NJ (1973).
9. Nielson, N. R., Ruder, B., Madden, J. D. and Wong, P. J., Computer System Integrity, SRI International, Menlo Park, CA (1978).
10. Parker, Donn B., Crime by Computer, Charles Scribner's Sons, New York (1976).
11. Wong, K. K., Computer Security Risk Analysis and Control, Hayden Book Company Inc., Rochelle Park, NJ (1977).

U.S. GOVERNMENT PRINTING OFFICE : 1979 O - 297-362