

INPUT

March 8, 1982

Dear Client:

Enclosed is the first technology brief in your 1982 subscription to INPUT's Management Planning Program in Information Systems, Beyond 3081: The Large Systems Issue.

In the course of its ongoing research in support of this report and other projects, INPUT has become aware of certain performance characteristics of the IBM 3081 that are likely to have an adverse effect on system conversion experience if they are not factored into conversion plans. If this information does not concern you directly, please pass it along to your Operations Manager.

Early reports are that physical installations of the IBM 3081 are exceptionally smooth and trouble-free. User reactions to the installation of an IBM 3081 to replace an IBM 3033 are overwhelmingly favorable, as the improvement in system response time is quite perceptible.

Within IS departments, however, the feeling is growing that the IBM 3081 is not living up to expectations. In terms of raw power, each of the two dyadic 3081 processors is the equal of an IBM 3033 uniprocessor, but system throughput appears to be significantly--and disappointingly--below that of two IBM 3033s.

The shortfall in throughput relative to expectations is most apparent in a VM/370 environment, when an IBM 3081 processor complex replaces an IBM 3033 CPU, with no other modification to the system configuration; i.e., a simple box-for-box CPU swap. In INPUT's opinion, the reasons for the shortfall may account for lower than expected performance in other operating system environments as well.

Put succinctly, a user who expects to replace two IBM 3033 VM systems with one IBM 3081 VM system, as the hardware performance specifications would leave one to expect, will be in serious trouble. VM/SP on the IBM 3081 currently just does not run very well.

The disparity between theoretical and currently realizable actual performance is directly attributable to the hardware architecture changes discussed in the accompanying report. In November 1980, IBM introduced the IBM 3081 Model Group D (MG D) with virtual machine assist (VMA, or VM assist) as a standard hardware feature, and concurrently announced the availability of VM assist as RPQ feature EJ1156 on the IBM 3033. VM assist is used extensively by VM/SP. Among other things, VM assist directly executes at least 30 privileged instructions, in part or totally, that are simulated by the command processor (CP) component of VM in systems that

do not have VM assist. The time used by VM assist is problem state time, and is so reflected in virtual machine time accrual. Thus, a decrease in CP time--which is absorbed as system overhead in VM systems without VM assist--is offset by an increase in virtual CPU time. However, the increase in virtual CPU time is not necessarily proportionate to the decrease in CP time.

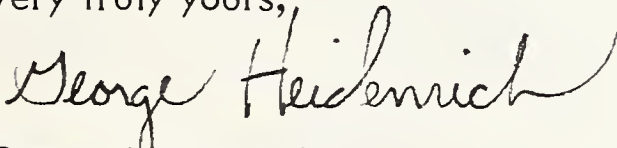
Thus, the existence of VM assist in the IBM 3081 will result in a disproportionate increase in billable virtual machine time relative to an IBM 3033 without VM assist.

Additionally, if an IBM 3033 job stream is executed without modification on an IBM 3081, the improved performance of the dyadic processors will result in twice as many I/O requests occurring in the same time as compared with their frequency on an IBM 3033. Therefore, without some "fine tuning" to accommodate the resultant mismatch between processor and I/O channel speeds, replacement of only the CPU will result in a bottleneck in the system I/O, with predictable degradation in system throughput.

INPUT understands that IBM is aware of the problem, and is modifying three specific components of VM, namely, free storage management, the I/O dispatcher, and the demand paging algorithm. The implicit intent is to restore a balance between the processors' speed and the I/O channels, especially in the area of demand paging, which is the prime suspect in terms of throughput degradation.

INPUT intends to keep its clients informed on a timely basis of developments in this area.

Very truly yours,



George Heidenrich  
Vice President

GH:ml

Enclosure



Digitized by the Internet Archive  
in 2015

<https://archive.org/details/vendorwatchrepor19unse>

**INPUT  
MANAGEMENT  
PLANNING PROGRAM  
IN  
INFORMATION SYSTEMS**

**VENDOR WATCH REPORT**

**NEW ISSUES IN COMPUTER SECURITY**

**DECEMBER 1982**

## MANAGEMENT PLANNING PROGRAM IN INFORMATION SYSTEMS

**OBJECTIVE:** To provide managers of large computer and communications systems with timely and accurate information on developments which affect today's decisions and plans for the future.

**DESCRIPTION:** Clients of this program receive the following services each year:

- |   |   |   |
|---|---|---|
| <ul style="list-style-type: none"> <li>● <u>Impact/Planning Support</u> for users of projected systems over the next five years.</li> </ul> | <div style="border: 1px solid black; padding: 2px;"> <p>U-V29<br/>1982</p> <hr/> <p style="font-size: small; color: blue;">AUTHOR</p> <p>NEW ISSUES IN COMPUTER SECURITY</p> <hr/> <p style="font-size: small; color: blue;">TITLE</p> </div> | <p>with the impact on developments over</p>                   |
| <ul style="list-style-type: none"> <li>● <u>Technology and major computer, communications marketing strategies.</u></li> </ul>              |   | <p>probable moves of , data base/data networks, and other</p> |
| <ul style="list-style-type: none"> <li>● <u>Residual Value</u> of mainframe and</li> </ul>  | <p>U-V29<br/>1982</p>   | <p>values of major</p>  |
| <ul style="list-style-type: none"> <li>● <u>Annual Planning</u> long-term plan classification. of the year.</li> </ul>                      |   | <p>both short- and major industry the second half</p>         |
| <ul style="list-style-type: none"> <li>● <u>Conference - National</u> in the fall quarter.</li> </ul>                                       |   | <p>venient location</p>                                       |
| <ul style="list-style-type: none"> <li>● <u>Inquiry Service</u> as-needed basis.</li> </ul>   |   | <p>arch staff on an</p>                                       |

**RESEARCH METHOD** in computers, communications, and

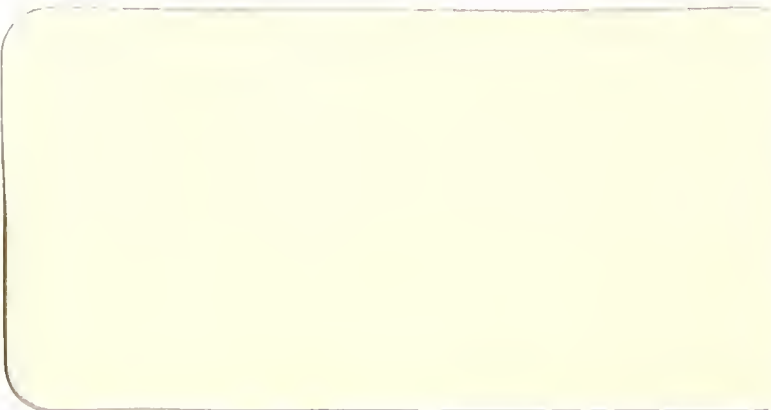
- Research topics discussed with client representatives
- Research for the universities, including users, vendors,
- Conclusions developed by professional staff in support of INPUT's
- Professional staff supporting this program average nearly 20 years of experience in data processing and communications, including senior management positions with major vendors and users.

For further information on this report or program, please call or write:

INPUT  
 Park 80 Plaza West-1  
 Saddle Brook, NJ 07662  
 (201) 368-9471

or

INPUT  
 P.O. Box 50630  
 Palo Alto, CA 94303  
 (415) 493-1600 Telex 171407



**INPUT**

**INFORMATION  
SYSTEMS PROGRAM**

VENDOR WATCH REPORT

NEW ISSUES IN COMPUTER SECURITY

DECEMBER 1982





# NEW ISSUES IN COMPUTER SECURITY

## CONTENTS

	<u>Page</u>
I INTRODUCTION .....	1
A. Background	1
B. Report Scope	6
II MANAGEMENT SUMMARY .....	9
A. What Does Security Include?	9
B. Emerging Security Threats	9
C. Recommended Actions	11
1. Risk Analysis	12
2. Counter-Penetration Program	14
3. Megadisaster Planning	14
4. Actions Requiring Little Or No Analysis	14
5. Actions Requiring The Selection Of Alternatives	16
III PHYSICAL THREATS .....	19
A. Threats And Solutions	19
B. Alternate Data Centers	25
C. Megadisaster Requirements	28
IV UNAUTHORIZED FILE ACCESS .....	37
A. The Scope Of The Problem: Thieves And Joy Riders	37
B. Control Mechanisms	41
C. Potential Technical Solutions	43
1. System Penetration	43
2. Interception	46
a. Cryptography	47
b. Fiber Optics	47
c. Decentralized Data Processing	48
D. Summary	49
E. A Counter-Penetration Program	49
V ASSESSING AND DEALING WITH RISK .....	53
A. Approximate Risk Analysis	53
B. Insurance	61

# NEW ISSUES IN COMPUTER SECURITY

## EXHIBITS

		<u>Page</u>	
I	-1	Reasons For Changing Backup Arrangements	2
	-2	Degree Of Senior (Non-Data Processing) Management Concern About Disaster Recovery	3
	-3	Disaster Recovery Service Decision Maker	4
II	-1	Security Planning Components	10
	-2	Determining Relative Importance Of Security Initiatives	13
III	-1	Physical Threats: Duration, Cause, And Effect	21
	-2	Physical Threats And Sources Of Protection	23
	-3	Relative Cost Of Sources Of Physical Protection	24
	-4	Access Time Requirements To Alternate Data Center Site In Case Of A Disaster	26
	-5	Trends In Backup Arrangements	29
	-6	Satellite Communication Alternatives	30
IV	-1	Unauthorized Data Access	40
	-2	Comparison Of Biometric Control Systems	45
V	-1	Severity Scales For Effects Of Disruptive Situations	56
	-2	Effects Of Disruptive Situations (Worksheet)	58
	-3	Impact Of A Computer Outage On Different Types Of Applications	59
	-4	Data Threat Worksheet	62

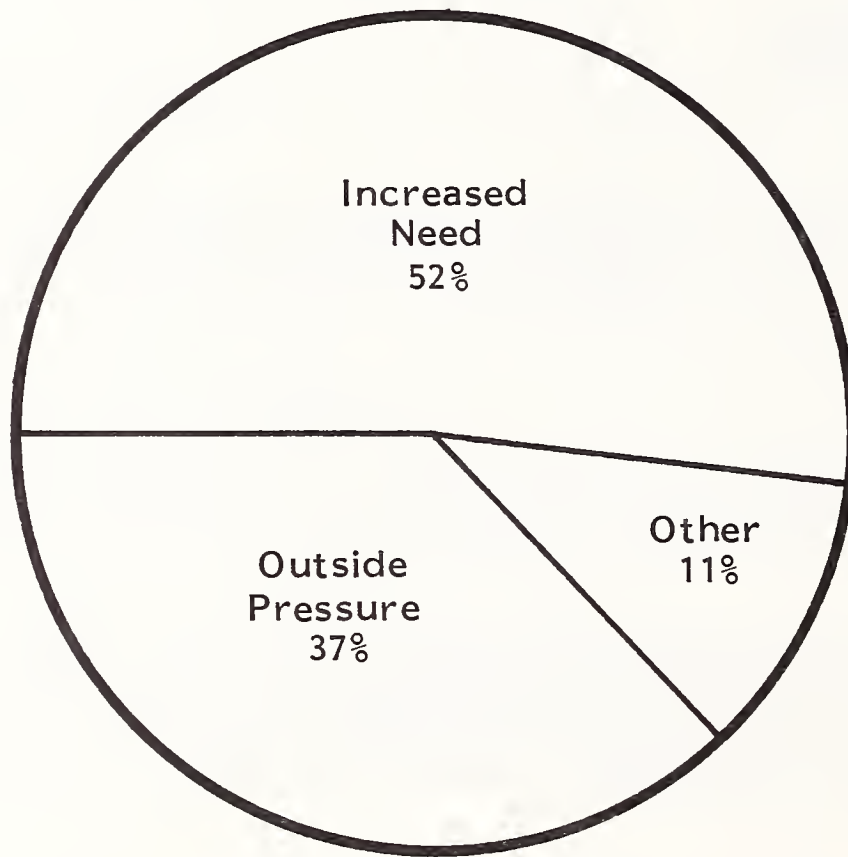
## I INTRODUCTION

### A. BACKGROUND

- Data processing security and its most prominent component, disaster recovery planning, are key objectives for relatively few information system (IS) departments.
  - In INPUT's 1982 user survey, for example, only 6% of respondents considered security a key issue.
  - Partly, this is because security plans and actions are often spurred by non-IS pressure and prompting, generally by auditors and sometimes upper management, as shown in Exhibit I-1.
    - In fact, non-IS managers have a surprisingly high degree of concern over one of the key areas of security, disaster recovery, as shown in Exhibit I-2. They are, however, unfamiliar with many other security-related issues.
    - Thus, it is not surprising that non-IS managers usually make the final decision in selecting a disaster recovery service, as shown in Exhibit I-3.

EXHIBIT I-1

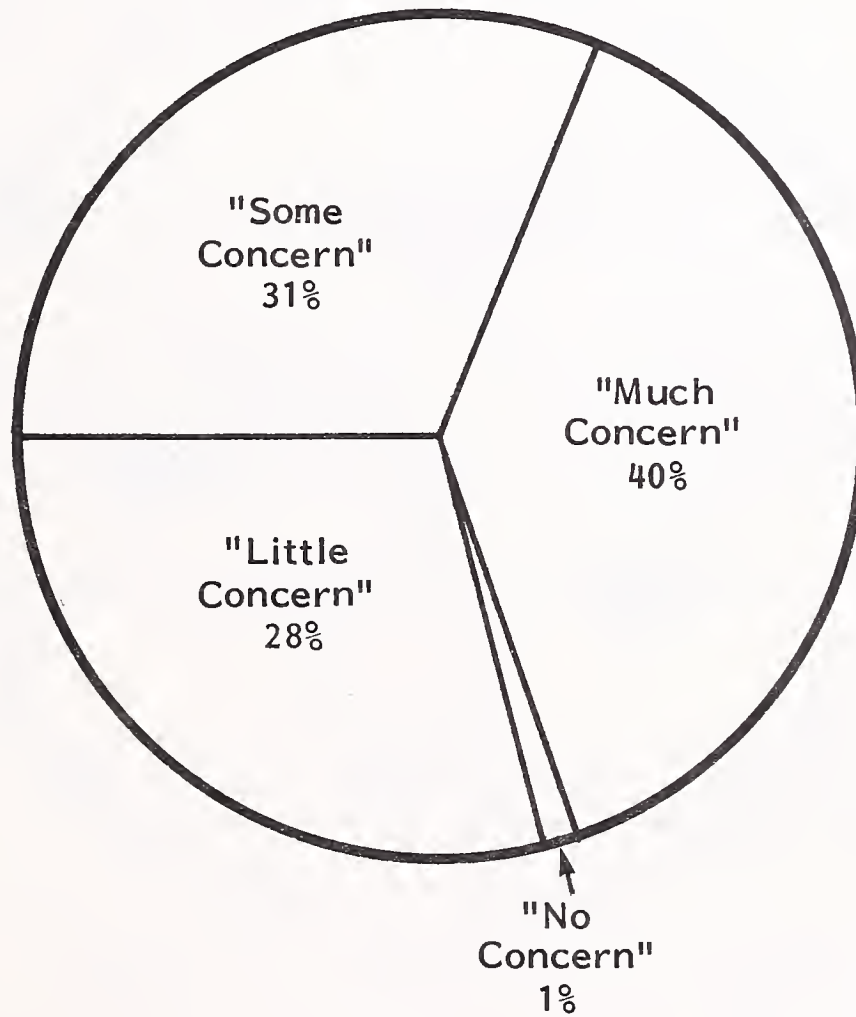
REASONS FOR CHANGING BACKUP ARRANGEMENTS  
(percent of respondents)



SOURCE: INPUT Study

EXHIBIT I-2

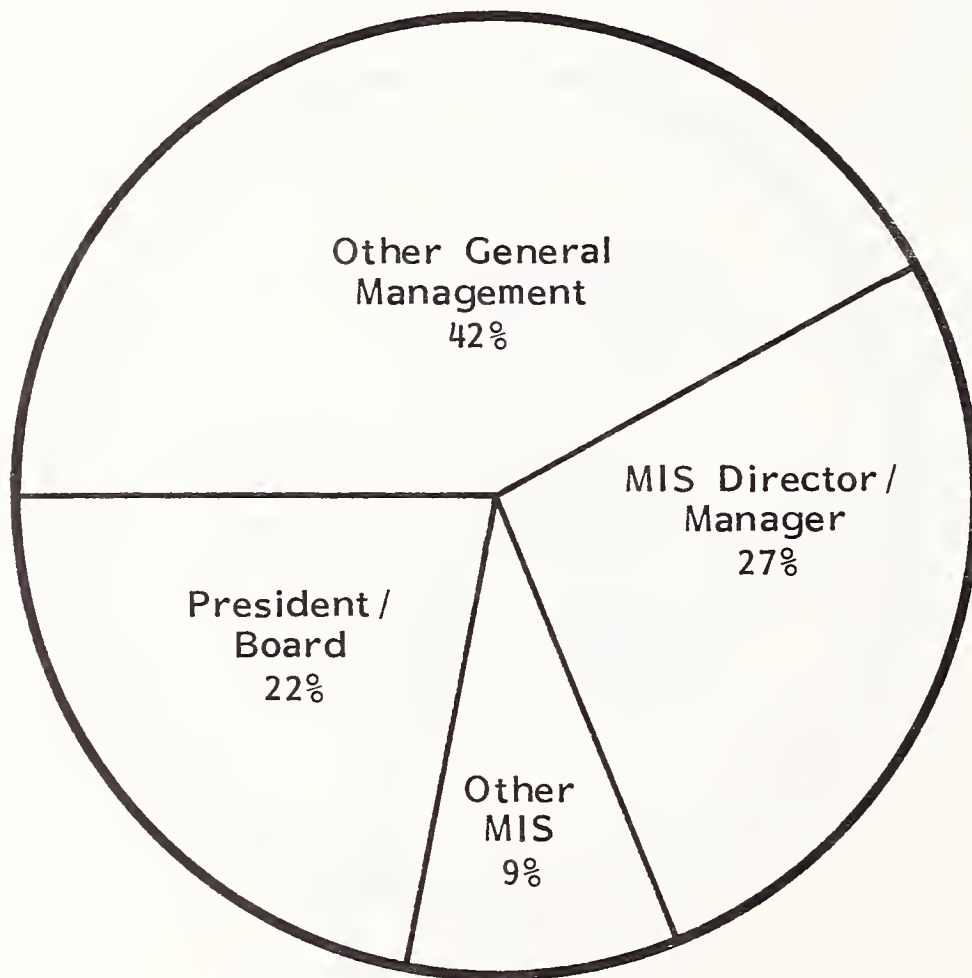
DEGREE OF SENIOR (NON-DATA PROCESSING)  
MANAGEMENT CONCERN ABOUT DISASTER RECOVERY  
(percent of respondents)



SOURCE: INPUT Study

EXHIBIT I-3

DISASTER RECOVERY SERVICE DECISION MAKER  
(percent of respondents)



SOURCE: INPUT Study

- There is often a lag in awareness among both IS and user staff over how dependent key operations have become on data processing.
- In addition, security issues often have to give way to more immediate concerns such as meeting schedules, satisfying users, or keeping qualified personnel.
- However, security issues are of ongoing importance to many IS organizations, as indicated by the total weighted vote in the client ballots for the topics for the 1982 Information Systems Program.
- In INPUT's experience, the general lack of high priority given to security and the sometimes inadequate security planning which follows has several causes:
  - Security breaches are seemingly infrequent and, when they occur, are often not publicized. Even a large IS organization may often be aware of only a few, apparently minor, incidents in a period of several years.
  - There is no commonly accepted definition of what "security" encompasses.
    - For some, it means only physical security, sometimes access control, more often, preventing or recovering from a disaster.
    - Others take a more general view, relating security to threats of other kinds (dishonesty, faulty power supplies, data bases contaminated in error, etc.).
    - This elasticity has prevented a broadly accepted definition of security problems and solutions from emerging.
- In INPUT's interviews with IS staff responsible for security it was clear that in many cases security planning is not effective.

- In many organizations, neither IS management nor general management takes an informed, continuous interest in security; rather, responsibility is delegated to a staff group (often a single person).
- The goal of too much security planning is to produce a document to satisfy auditors.
  - In one large bank, for example, a basic component of the security plan is to have its hundreds of on-line offices revert to manual methods if the main computer installation becomes inoperative for a lengthy period of time.
  - Its computer installation is on an upper floor of an office building and has no fire suppression system. Backup is an (untested) mutual assistance agreement with a nearby company; only batch work would be run.
  - When asked how well manual backup worked, the bank officer replied: "We wouldn't dare test it, it would be far too disruptive. Too many of our people now have experience only on the on-line system."
- Many IS organizations have doubts about the effectiveness of their own security planning. A significant portion of security planners interviewed did not show full confidence in their efforts. This was manifested in many ways, the most striking of which was the semi-joking reply by several respondents to what they would do in the event of a disaster actually occurring. Their answer: "Update my resume."

## B. REPORT SCOPE

- The purpose of this report is to put security issues in a single planning context.



The report will focus on what INPUT has identified in its research as the key issues and actions which should receive attention from IS management.

- There are other areas where there is a consensus, based on experience and analysis, that action is necessary and effective. These areas will be noted; where action has not already been taken by an IS organization, serious consideration should be given to immediate implementation.
- The bulk of the information and recommendations in this report are based on recent special consulting assignments in the security area which have given INPUT insights into IS departments' and vendor organizations' needs and plans.
  - In addition, INPUT has investigated new products and services which could at the least prove useful and may represent potential breakthroughs.
- The remainder of the report is organized as follows:
  - Chapter II is a summary of the key findings and recommendations.
  - Chapter III examines physical threats and solutions, with special attention paid to the "megadisaster."
  - Chapter IV looks at the more subtle problems associated with unauthorized data access. Two relatively new approaches to dealing with these problems are discussed:
    - Biometric access control.
    - A counter-penetration program.
  - Chapter V introduces the idea of an approximate analysis of risk as a means of understanding the seriousness of security problems and the costs and benefits of dealing with these problems.



## **II MANAGEMENT SUMMARY**

### **A. WHAT DOES SECURITY INCLUDE?**

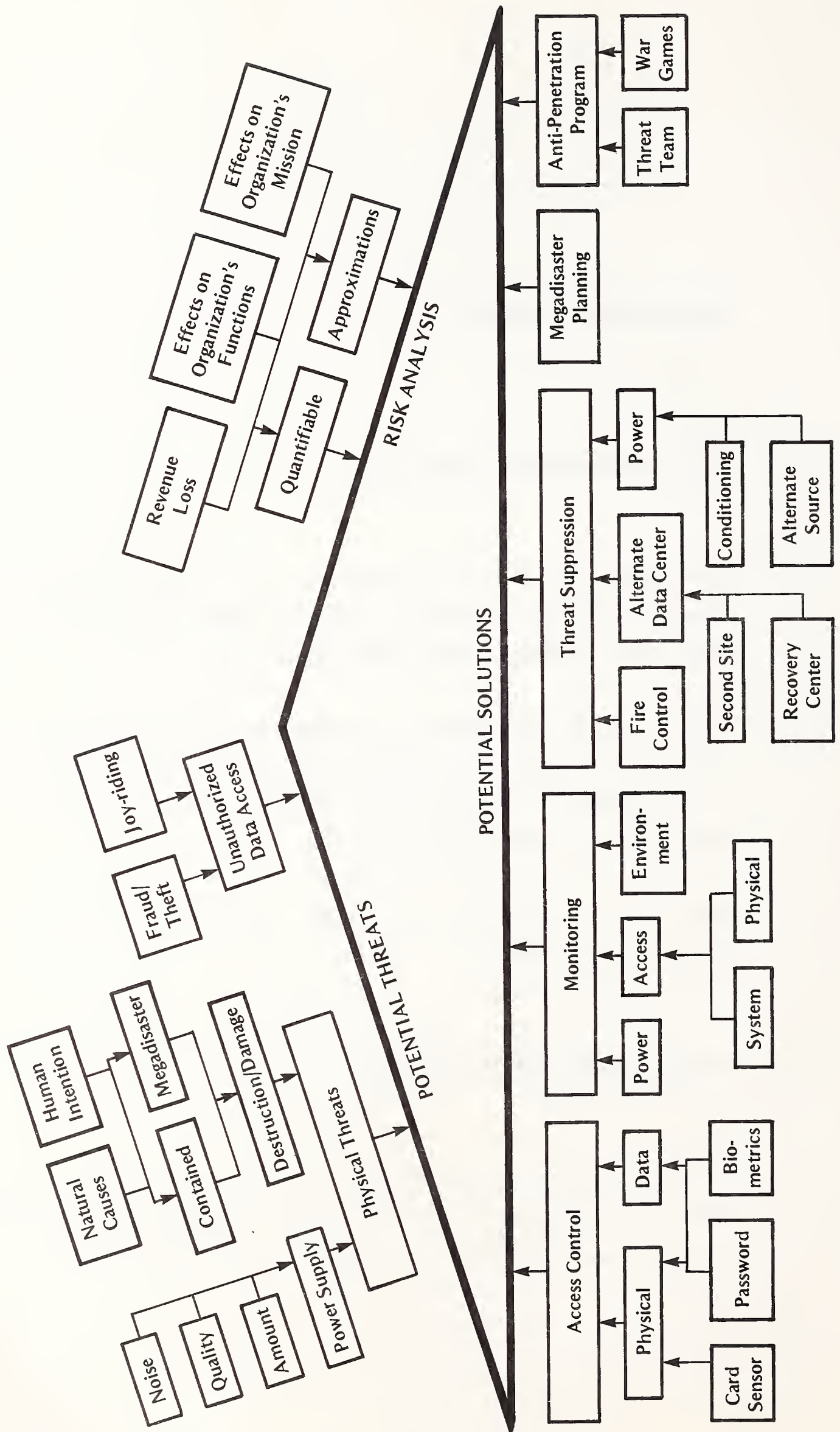
- Data processing security has suffered from incomplete and sometimes conflicting definitions as to what is or is not included in the term "security." This has hindered planning as well as effective action.
- INPUT's research and analysis have demonstrated the interrelation of security threats and solutions. Since both threats and solutions are potentially limitless it is necessary to introduce risk analysis as a third component, so that resources can be intelligently allocated.
- Exhibit II-1 summarizes the principal components of security threats, solutions, and risk analysis.

### **B. EMERGING SECURITY THREATS**

- One reason data processing security has languished is that until now security threats have been conventional (fire, etc.), infrequent, and would not have had a significant effect on many firms even if they had occurred.

EXHIBIT II-1

SECURITY PLANNING COMPONENTS



- Computer systems are becoming more important even if corporate awareness has not always kept up with reality.
  - Threats are becoming more expensive, but most organizations have no way of showing this.
- Because of the increased complexity of computer systems, they are easier to penetrate and more difficult to defend. The attraction of penetration is constantly growing:
  - Thieves wish to steal. While the technological component of most computer thefts is low, it is bound to increase.
  - Equally worrisome are the "joyriders" who just want to show that they can do it.
- Most firms have some sort of disaster plan (possibly ineffective), but very few know how they would respond to a "megadisaster," i.e., one regional in scope.
  - While the odds of a megadisaster occurring are small, they are not much smaller than those for a more limited disaster, as far as a single data processing center is concerned.

### C. RECOMMENDED ACTIONS

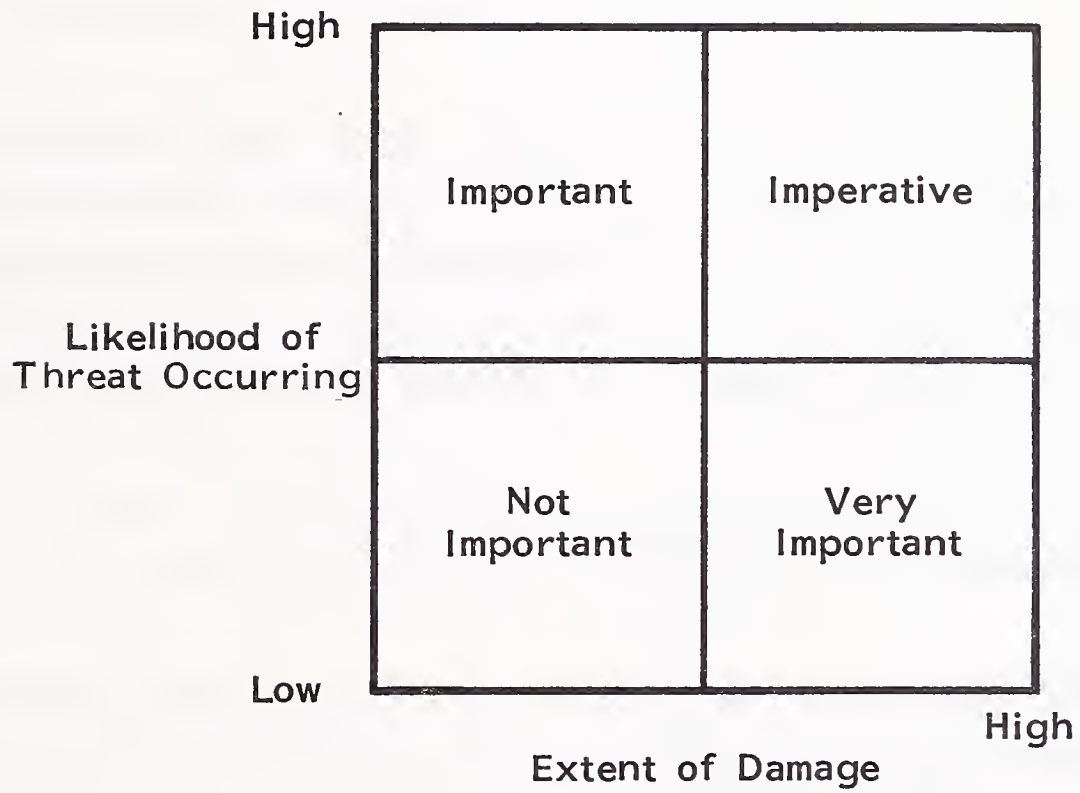
- Many aspects of computer security can be delegated to IS security staff once overall policy has been set. However, there are three very important areas that require the participation of user staff: risk analysis, a counter-penetration program, and megadisaster planning. None of these initiatives is in widespread use, but they are key steps in determining the overall direction of the IS security program.

## I. RISK ANALYSIS

- Personnel in most firms, especially IS staff members, are unfamiliar with the principles of risk analysis or are hesitant to use the technique.
- In addition, conventional risk analysis has generally proved unsatisfactory in a data processing environment.
  - The probability of critical events occurring cannot be easily or accurately determined (e.g., incidence of fraud or hardware disasters).
  - Similarly, the potential dollar loss from these events is difficult to quantify and some important effects of computer security breaches (e.g., loss of efficiency) are virtually impossible to quantify.
- However, without some kind of evaluation of risks and costs a proper security program cannot be devised.
- Data processing security requires "approximate" risk analysis. This replaces, where necessary, quantifications with verbal descriptions; e.g., the likelihood of an event occurring is "very low," but the impact on the organization would be "very high."
  - Prime risk areas include threats which interfere with machine operation as well as those affecting data integrity.
  - Threats can have effects on revenues, the internal functioning of the corporation, and its mission.
- The security program itself should focus on areas where the likelihood of a threat happening is the highest and where the damage would be most severe, as shown in Exhibit II-2.

EXHIBIT II-2

DETERMINING RELATIVE IMPORTANCE OF SECURITY INITIATIVES



## 2. COUNTER-PENETRATION PROGRAM

- Too many aspects of existing security programs are passive or reactive. This is especially true of security problems which arise from people who penetrate the system for either financial gain or personal reasons.
- Threat teams should be organized to review current procedures and financial controls. The team should be made up of employees from different areas who would hypothesize how the system (both manual and computer components) might be beaten and what steps should be taken to close gaps.
- War Games: Small groups of IS technical staff should be given assignments to try to gain access to the operating system and critical data surreptitiously. The lessons gained can be used to strengthen the system, as required.
  - An alternate approach is to engage outside specialists who attempt to penetrate the system.

## 3. MEGADISASTER PLANNING

- Most IS disaster planning assumes explicitly or implicitly that a data processing disaster will be limited in scope; in most cases the assumed maximum destruction is limited to the data center.
- A megadisaster would be regional in scope. IS cannot plan for a megadisaster by itself, but must have its plans thoroughly integrated with those of the entire corporation.
- A megadisaster is one of the few situations where variants of mutual backup agreements or shell sites can be justified.

## 4. ACTIONS REQUIRING LITTLE OR NO ANALYSIS

- There are several security-related actions which should be implemented in nearly every medium or large data processing facility. They have amply



proved their use and/or are the foundation for other security measures. Installations that have not made these implementations must, in effect, prove to themselves that there is no need.

- Smoke/fire/water detectors: Fire and water are obvious hazards and by far the most common reason for computer center destruction.
- Halon Fire Suppression System: Safe and effective, Halon can put out most fires at an early stage and greatly reduce the chance of water damage from fighting a fire; water is usually more of a danger than the fire itself.
- Electric Power Monitoring: This is critical for understanding the magnitude and solution to problems in power supply. Without monitoring it is not possible to establish an appropriate level of power backup and quality assurance. Many data centers have an inappropriate type of power backup because they did not monitor before committing themselves to a course of action.
  - Besides "micro-monitoring" of site power, IS should "macro-monitor" the regional electric power situation.
- Physical Access Control: A locked door/card entry system has become a symbol of data processing security. While it is often not possible to quantify its benefits, such a system is desirable because it usually enhances employees' sense of safety.
- Testing: All backup systems should be tested on a regular basis, especially those that require participation by non-IS staff. Some tests should take place without prior notice.
- Off-Site Data Set Storage: Copies may have to be stored at more than one off-site location (see "Megadisaster" in Chapter III).

## 5. ACTIONS REQUIRING THE SELECTION OF ALTERNATIVES

- Virtually every data processing installation should have some kind of security initiatives in the following areas:
  - Off-site recovery.
  - Electric supply quality assurance.
  - Data access control.
  - Insurance.
  - Written security plan.
- However, these are definitely not "one size fits all" problems. The matching of risk levels and appropriate actions is critical.
- Off-Site Recovery: The basic alternatives are the use of a commercial recovery center or establishing a twin site. A twin site requires a multi-million dollar investment and the incremental operating costs will be considerably more than the annual fee for a commercial recovery center. However, access to a commercial recovery center cannot be guaranteed. Consequently, where risk analysis shows a very high dependence on continued data processing, a twin site may be required.
- Electric Supply Quality Assurance: The required solutions may range from a simple voltage surge controller to an uninterruptable power supply plus diesel generator; one solution may cost 100 times more than the other. Monitoring and risk analysis will show the level of protection needed.
- Data Access Control: Passwords are inadequate beyond a certain point. Biometric controls based on unchangeable personal characteristics (voice, fingerprints, etc.) may be needed to guard critical parts of the system.

- Insurance is not a replacement to any other type of security; dollars alone will not quickly replace a destroyed computer in the absence of prior planning. However, insurance can be a useful supplement to other security efforts.
  
- A Security Plan is definitely not a mechanical, workbook exercise but is the documentation of the various security options chosen that are suitable for a particular organization at a particular time.
  - Many of the widely available outlines are quite suitable as checklists to make sure that items have not been forgotten, but they cannot replace the individual analysis required in a particular organization setting.
  
  - Security planning is much more comprehensive than a disaster recovery plan, although disaster recovery is certainly a very important component of security planning, as shown in Exhibit II-1.



### III PHYSICAL THREATS

#### A. THREATS AND SOLUTIONS

- Most physical threats to a data center come from natural causes; i.e., poor quality electric power or a natural disaster (fire, flood, etc.).
  - People may trigger an otherwise natural event (e.g., power failure, fire).
  - In rare cases, people may directly damage computers.
  - A partial remedy is some form of perimeter control (the classic card key or in the most secure settings a personalized radio transmitter such as the "Mastiff" by Mastiff Systems U.S.).
    - The larger threat is from disgruntled personnel, either about to leave or just out of employee status.
    - There is not a great deal that can be practically done to prevent this kind of problem.
- While many different kinds of physical threats are possible, their effects generally fall into one of three categories:

- Electrical line disturbance.
  - Inoperable data center (either a short or a lengthy outage).
  - Destroyed data center (i.e., permanently inoperable).
- Exhibit III-1 shows the threat-outage time relations in more detail and the potential effects on data and equipment.
  - Certain actions should be taken to deal with physical threats with little or no analysis needed. They are obvious steps or are the foundation for other security decisions. They include:
    - Smoke/fire/water detectors.
    - Halon fire control system.
    - Electric power monitoring.
  - With the major exception of a total disaster, the physical threat decisions mainly revolve around the kind of electric power protection that should be obtained.
  - This makes power monitoring especially critical:
    - It provides data for negotiating with the local electric utility.
    - It provides data for quantifying input data for risk analysis.
    - These data define what power problems must be solved.
      - Numerous data centers have received either too much or too little electric power backup or conditioning because they did not understand what their problems were.

## PHYSICAL THREATS: DURATION, CAUSE AND EFFECT

DURATION OF OUTAGE	CAUSES (examples)	EFFECTS		
		STORED DATA LOSS	EQUIPMENT	
None - Line Disturbance (noise)	Microwave, Radar, Electrical Storm	Random	Minor Effects	
None - Line Disturbance (transients)	Lightning, Machinery On-Line, Utility Transformer Step Up	Random	Equipment on Affected Line May be Damaged	
Momentary Outage (under 0.5 seconds)	Voltage Sag, Area Feeder Failure	In-Process Data May be Lost	Disk Crash Possible	
Brief Outage (0.5 seconds to 15 minutes)	Voltage Sag, Local Blackout, Area Feeder Failure, Cooling Failure	Data In Process and on Crashed Disks may be Lost	Disk Crash Possible	
Long Outage (15 minutes to several hours)	Regional Blackout, Building Feeder Failure (if single feed), Cooling Failure	Data In Process and on Crashed Disk may be Lost	Disk Crash Possible	
Very Long Outage (more than several hours)	Regional Blackout, Minor Fire, Cooling Failure	Much Data may be Lost	Disk Crash Possible; Other Equipment May be Damaged or Destroyed	
Permanent Outage	Major Fire, Flood	Total	Total	

- Besides "micro-monitoring" of site power, IS should "macro-monitor" the regional electric power situation. Most utilities now have over-capacity and have stopped building new facilities. By the end of the 1980s, there may be regional shortages again; it will be easy to forecast this several years ahead of time and take necessary steps (e.g., install a diesel generator).
- The particular outage time periods in Exhibit III-1 correspond to the dividing points in effective protection of different kinds of protective equipment.
  - Exhibit III-2 shows to what extent each type of protective equipment can deal with a particular type of threat.
  - It demonstrates the need to accurately monitor electric input so that problems and solutions are correctly matched.
- Exhibit III-3 shows that the differences in cost between the different types of protection are nontrivial, especially since a battery/diesel generator installation can cost well over \$1 million.
  - The difference in installation cost between the newer transformer-based line conditioners and the older motor generators is also true for operating costs: transformer-based equipment is more efficient at partial loads.
  - However, knowing the distribution of the different kinds of outage and the costs of solutions does not in itself provide enough information with which to make a decision on the level of protection needed.
- The effects on critical application systems must be assessed. For example, an organization may find after analysis is complete, that there would be no serious effects if an outage of several days were suffered. In that case line conditioning, at most, would be required.



EXHIBIT III-2

PHYSICAL THREATS AND SOURCES OF PROTECTION

THREAT	AMOUNT OF PROTECTION, BY SOURCE					
	REGULATOR SURGE PROTECTOR	LINE CONDITIONING		BATTERY (UPS)	BATTERY AND DIESEL GENERATOR	ALTERNATE DATA CENTER
		TRANSFORMER-BASED	MOTOR GENERATOR			
Line Disturbance (noise, transients)	50%	100%	100%	100%	100%	0
Momentary Outages (0.5 seconds)	0	100	100	100	100	0
Brief Outage (0.5 seconds to 15 minutes)	0	0	0	100	100	0
Long Outage (15 minutes to several hours)	0	0	0	Partial*	100	0
Very Long Outage (greater than several hours)	0	0	0	Partial*	100	100%
Permanent Outage	0	0	0	0	0	100

\*Permits Orderly Power-Down

EXHIBIT III-3

RELATIVE COST OF  
SOURCES OF PHYSICAL PROTECTION

SOURCE	RELATIVE INSTALLATION COST*
Regulator or Surge Protector	0.05 - .2
Transformer-based Line Conditioning	0.2 - 0.3
Motor Generator Line Conditioning	0.35 - 0.45
Battery (UPS)	0.7 - 0.8
Battery and Diesel Generator	1.0
Alternate Data Center	0.1 to over 2.0

\* Battery/Diesel Generator Combination = 1.0

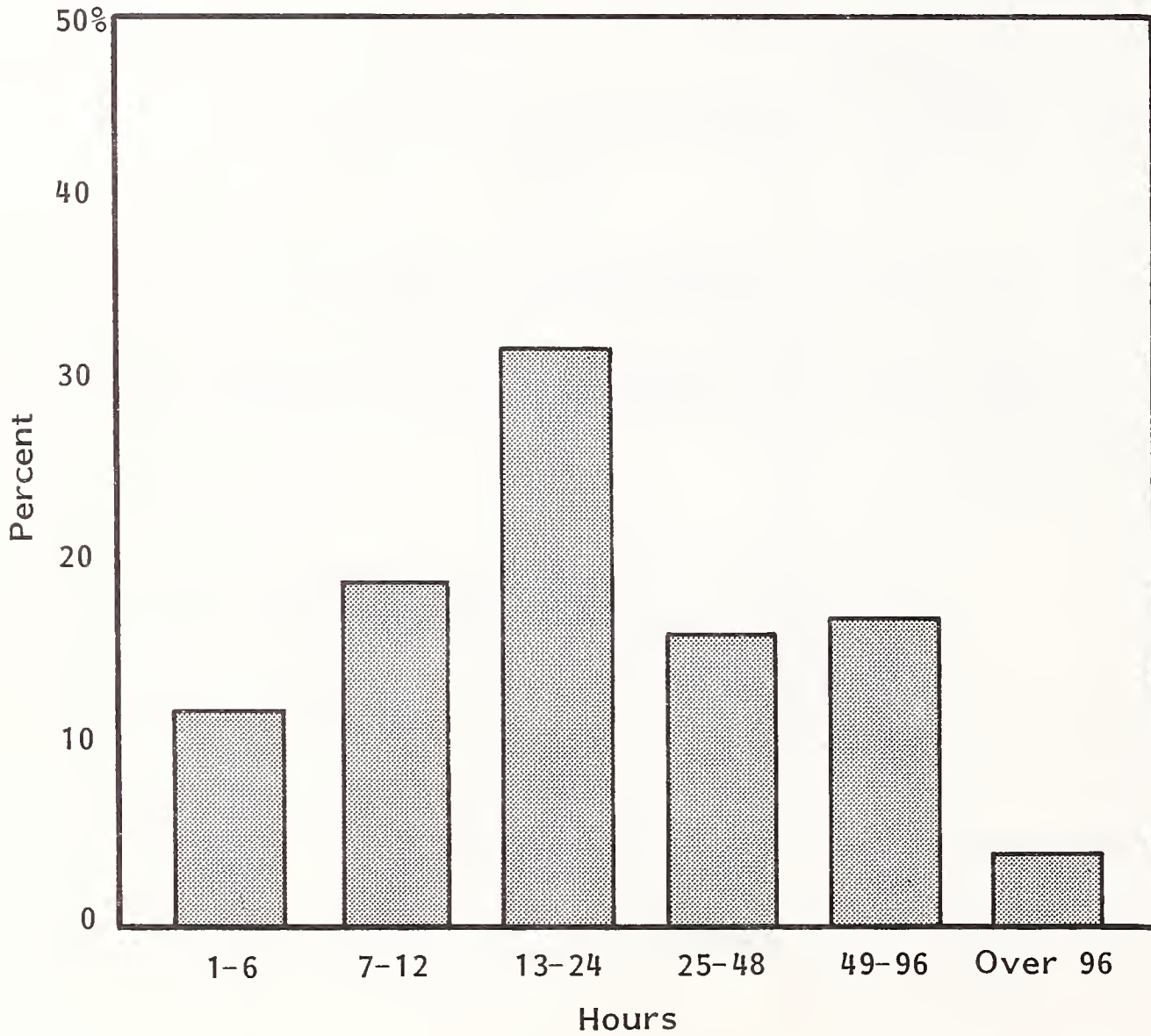
- Assessing these effects is central to risk analysis and is discussed in Chapter V.

## B. ALTERNATE DATA CENTERS

- The wide variation in costs for an alternate data center, as shown in Exhibit III-3, reflects the choices between:
  - A commercial recovery center (e.g., Sungard, Comdisco) with an annual standby fee of \$40,000 to \$100,000.
  - A second data center, specially built in another area for backup purposes. Even if the capacity of a second data center can be justified because of increased service requirements, the additional costs chargeable to its backup function will greatly exceed the costs of a backup service.
    - The two (or more) sites must each operate at considerably less than normal loads if a margin for backup is to be maintained. This will be difficult to do in the face of financial and user pressures.
- Why even consider building a second center?
  - Some very large EDP systems are too large to be able to use a recovery center.
  - Others cannot afford to be down for the hours it would take to be reestablished in the commercial recovery center, as shown in Exhibit III-4.

EXHIBIT III-4

ACCESS TIME REQUIREMENTS TO  
ALTERNATE DATA CENTER SITE IN CASE OF A DISASTER



Source: INPUT Survey

- Most importantly, there is no guarantee that a recovery center would be able to service a client. In a regional blackout, for example, many clients would want to use the recovery center at the same time. Some companies cannot live with even the smallest chance of this happening.
  - This is the Achilles' heel of commercial recovery centers: each center has about 100 clients signed up but could probably only support one or two at once.
  - The other problem that commercial recovery centers have is that they have never been used under "battlefield" conditions. No one can really say how they will perform.
- It should be stressed that if a second center is to have real backup importance it should be built in a different telephone and electricity grid.
  - One large IS department justified a second center partly on backup grounds. It is less than ten miles away from the primary data center.
- Most organizations are dependent on teleprocessing although they are not always aware of the degree to which they are dependent.
  - A majority do not feel that existing teleprocessing systems could be replicated in an emergency.
  - Many feel that 4800 band service would be adequate in an emergency.
- The increased use and dependence on on-line systems will be an increasingly vital disaster planning issue.

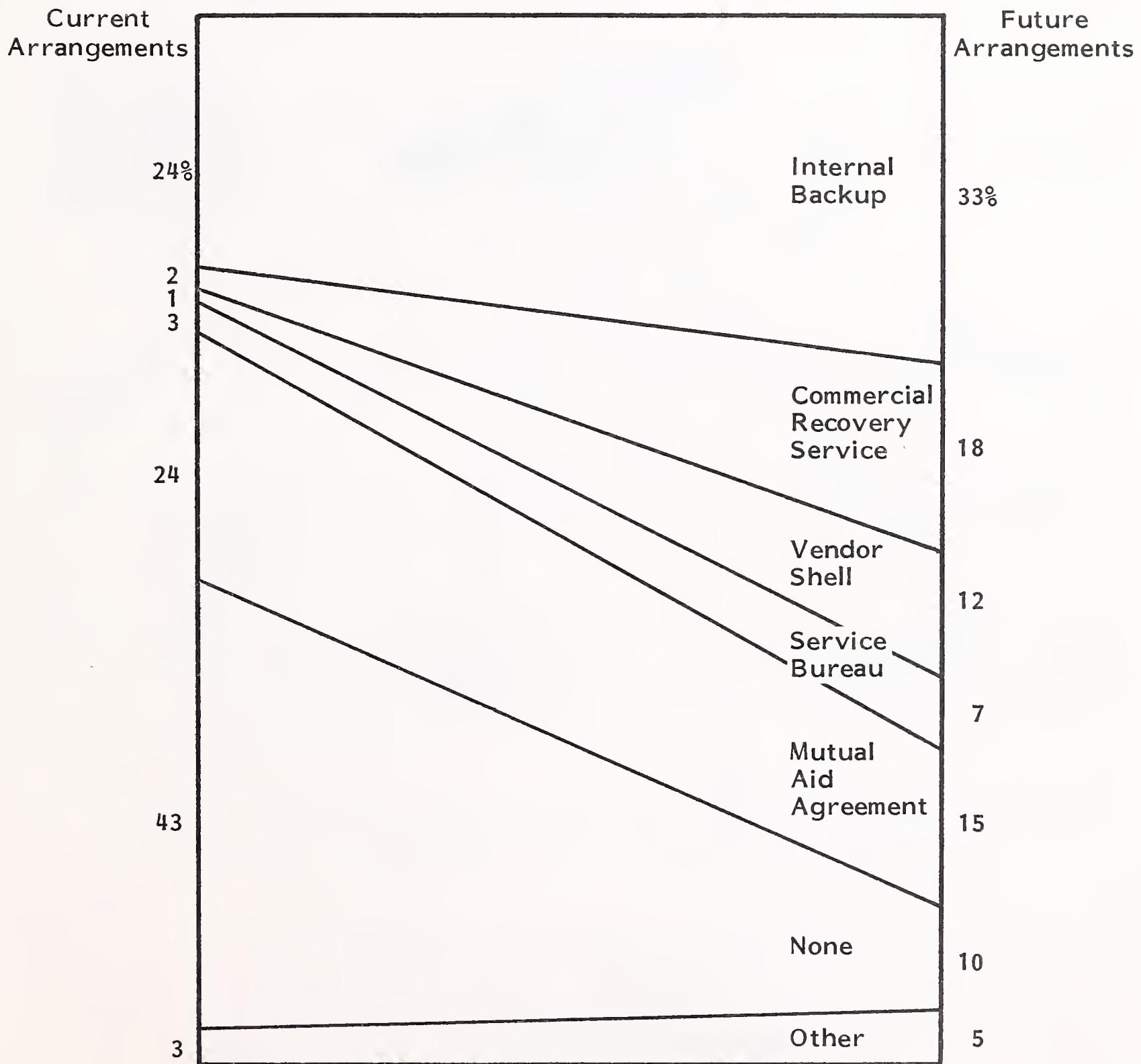
- It is important that both MIS and user management keep on top of changes in this area. Often, there is a "perceptual lag" between the actual importance and the assumed importance.
- In addition, there are significant problems associated with maintaining complete telecommunications networks with multiple focal points.
- Teleprocessing needs have caused MIS planning to look to guaranteed backup, either internal or an outside vendor, as shown in Exhibit III-5.
  - In most cases, shells (an alternate site with little or no hardware installed) and mutual aid agreements with local firms will not prove satisfactory.
- Advances in satellite technology and coverage continue to make second sites more feasible from a communication standpoint.
  - Satellite networks can, in principle, be redirected immediately to a second computer center, as shown in Exhibit III-6.
  - The satellite link would also make splitting processing between two locations somewhat more cost effective.

### C. MEGADISASTER REQUIREMENTS

- A major fire can totally destroy a data processing installation's capabilities and, in doing so, can threaten the existence of a firm. However, this is a "disaster" only to IS and, perhaps, the remainder of the organization.
- There is the possibility that a disaster of much greater dimensions could occur, one that would be "off-the-scale" of normal experience. Such a megadisaster would have the following characteristics:

EXHIBIT III-5

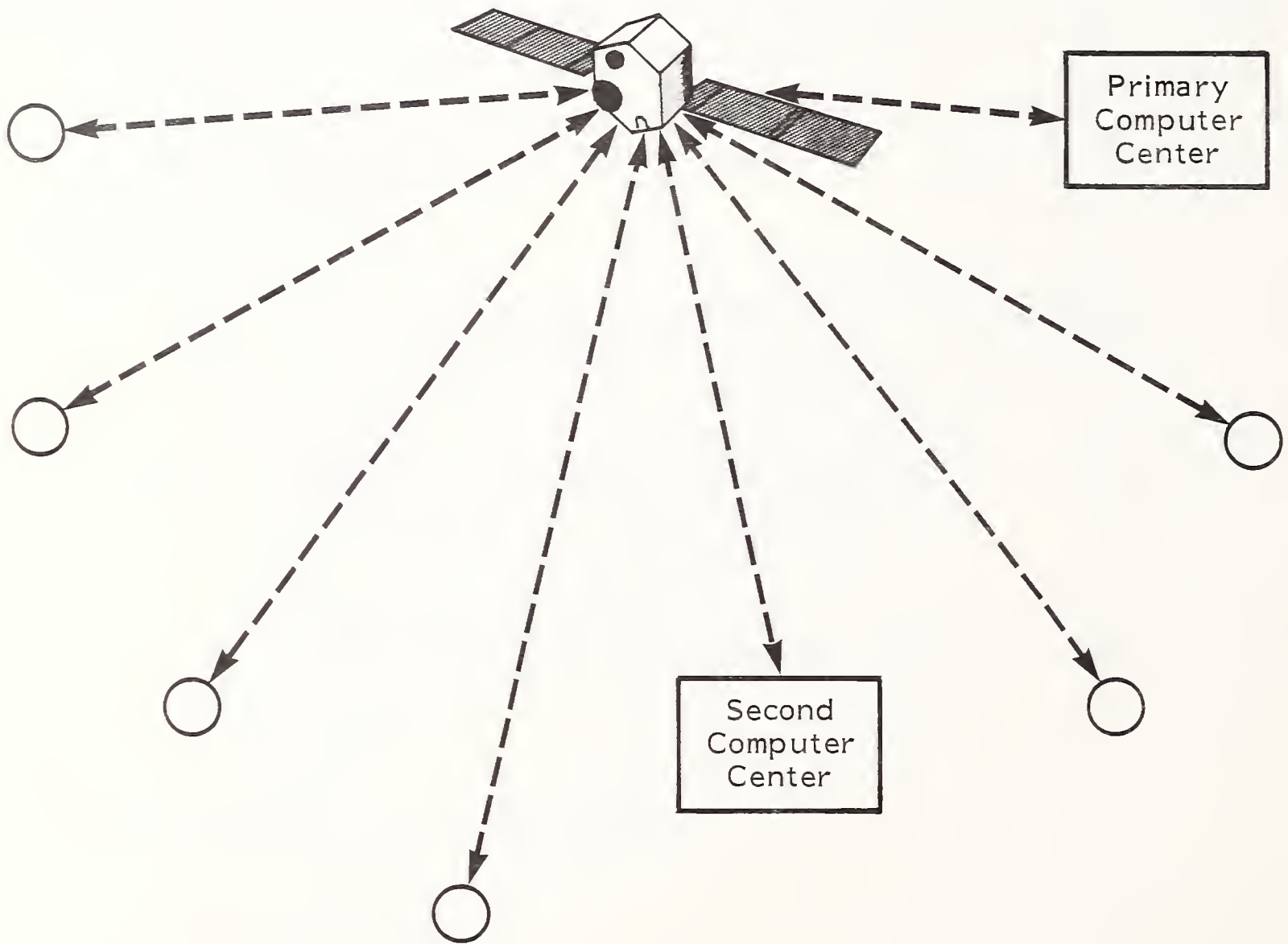
TRENDS IN BACKUP ARRANGEMENTS



Source: INPUT Survey

EXHIBIT III-6

SATELLITE COMMUNICATION ALTERNATIVES



○ ←-----→ Regional Concentrator



- Widespread, serious property destruction.
  - Lengthy disruption of normal life in a region.
  - Many key IS and corporate staff unavailable for a prolonged period.
  - Significant numbers of customers and suppliers affected (including utility and computer suppliers).
- This level of disaster could be caused by:
    - War or widespread civil disorders.
    - Atomic accident.
    - Natural disaster on the scale of the 1906 San Francisco earthquake and fire.
- How likely is such a megadisaster to occur? For some companies a megadisaster may be more likely to occur than a "normal" disaster (say, a fire that destroys the data center).
    - A data center may take a great deal of care to prevent "normal" megadisasters from occurring, reducing the already small odds against this happening.
    - On the other hand, there is nothing that an IS department can do to prevent a megadisaster, or even mitigate its immediate effects.
    - A firm located in the San Francisco area might find that by its efforts it had reduced the odds of "normal" disaster occurring to once every 50 years, while a serious earthquake would have the same likelihood of occurring in the next 25 years.

- This is speculation since disasters, like individual life expectancy, can be predicted, at best, in the actuarial sense, not for individual cases.
- The point is that all data centers have a potential (but small) chance of being involved in a megadisaster.
  - It is arguable that some locations may run greater risks than others (e.g., near the San Andreas Fault, in some foreign countries, downwind from nuclear reactors of a certain design, in some urban areas, etc.)
  - However, the numbers involved are both small and difficult to quantify. It is more conservative, and probably more correct, to say that, given present information, all data centers stand an equal chance of being involved in a megadisaster.
- Disasters of this magnitude cannot be planned for by IS alone. Any IS plan must take place within the context of a corporate-wide plan.
  - There would be no point in IS being able to cope with a megadisaster if the rest of the corporation had not made any plans.
  - In a megadisaster there will be a need to interact with other corporate units in a different way than in a disaster limited in its effects to IS alone.
    - Purchasing, for example, will not be able to focus on IS replacement needs.
    - Any telecommunication lines still available will have to be rationed for the use of the entire organization.
    - Top management time will be severely limited.

- Commercial recovery center facilities (e.g., Sungard or Comdisco) may be of only limited usefulness in a megadisaster.
  - Each backup facility will have many times more clients wishing to use it than it can handle.
  - National telecommunications may be severely impaired.
  - One or more of the commercial recovery centers may be within the disaster area, placing even more strain on remaining units.
  
- At the same time, recovery needs, allowable outages, and schedules will be much less demanding than in a disaster limited to a single firm or IS departments.
  - Everyone in a corporation will have many other things to be concerned with besides IS performance or availability.
  - A new scale of values and expectations will be automatically imposed.
  - Many competitors will be equally affected.
  
- In the megadisaster environment, a very basic level of data processing services will usually be quite sufficient for corporate needs. Examples of this approach include the following:
  - Centrally supplied end-user computing services could be discontinued.
  - Processing can be limited to applications needed for immediate operations (e.g., bills and receivables would be processed; fixed assets accounting would not be processed).
  - In some cases megadisaster processing would only have to approximate the result of normal processing.

- For example, payroll processing might not attempt to calculate a new payroll, but would print the last cycle's paychecks (and make adjustments later).
  - Where exact bills cannot be calculated, an average of the last 12 months bills would be billed on account. (Steps like this will be critical to maintain a satisfactory cash flow.)
- On-line services might be totally discontinued where feasible.
  - Many order entry situations can revert to manual transactions and batch input.
  - Where on-line files are used to look up and approve customer requests (e.g., check cashing), arbitrary limits can be used instead.
- Plain paper can be substituted for preprinted forms.
  - Masks can be used with laser printers.
  - Additional lines of "bare-bones" headings can be used instead.
- The preceding expedients assume, however, that a firm will have some computer capability available. This is not a simple issue since its own computer will be unavailable and quite likely that of its commercial recovery center.
- Obviously, a second site built a considerable distance away would be ideal. However, the logistical burdens that this additional distance would impose on normal day-to-day operations will make this choice daunting except for all but the largest firms.

- Many firms want to set up second sites too close to the main site for satisfactory backup in a much more limited disaster situation.
- Ironically, two normally discredited backup options become very viable in a megadisaster setting: mutual aid agreements and "shell" sites.
  - As discussed earlier, these two approaches are not satisfactory in today's on-line environment. However, after a megadisaster, expectations will be much lower, and variations of these approaches can serve as interim solutions.
- A mutual aid agreement can be made with a firm in another region. This is completely different from the traditional mutual aid agreement made with a nearby firm. The amount of computing resources to be made available should be realistic from both sides' standpoint.
  - Another division of the same parent organization would be ideal (assuming that the hardware and software configuration was reasonably compatible).
  - If an unrelated firm is used, then a reasonable level of payment should be provided for.
  - In any event, both sides should run regular tests on the other's machines.
- The "shell" should not be the normal empty shell, but should be at least partially filled. This is because it will be extremely difficult to obtain equipment after a megadisaster.
  - However, the equipment can be very cheap, obsolescent, and with a low market value.

- Special arrangements will have to be made to reduce maintenance expense for this standby equipment.
  - Several firms from different parts of the country can share expenses for preparing this kind of shell. The firms can supply part of their payment "in kind" by supplying facilities, equipment, etc.
- 
- Copies of software and data files should be stored in a secure location near the backup site. Copies stored in the same region, even in a secure facility, may not be accessible after a megadisaster.

## IV UNAUTHORIZED FILE ACCESS

### A. THE SCOPE OF THE PROBLEM: THIEVES AND JOY RIDERS

- Unauthorized data access is a human problem that expresses itself in technological terms. There are two kinds of people who try to illegally access files (including both data and program code), just as there are two kinds of people who steal cars:
  - The thief who wishes to obtain data of value or, more commonly, wishes to change data or program logic in order to obtain funds or other articles of value.
  - The "joy rider," who wishes to prove to himself or a small circle of friends that he is smarter than the computer system. His aim is usually to "trash" files or the operating system.
- It is very difficult, if not impossible, to identify these people before they are hired.
  - Internal thieves are often trusted employees prior to their unmasking. The financial or emotional problems that led them to adopt dishonest ways were unnoticed or overlooked.

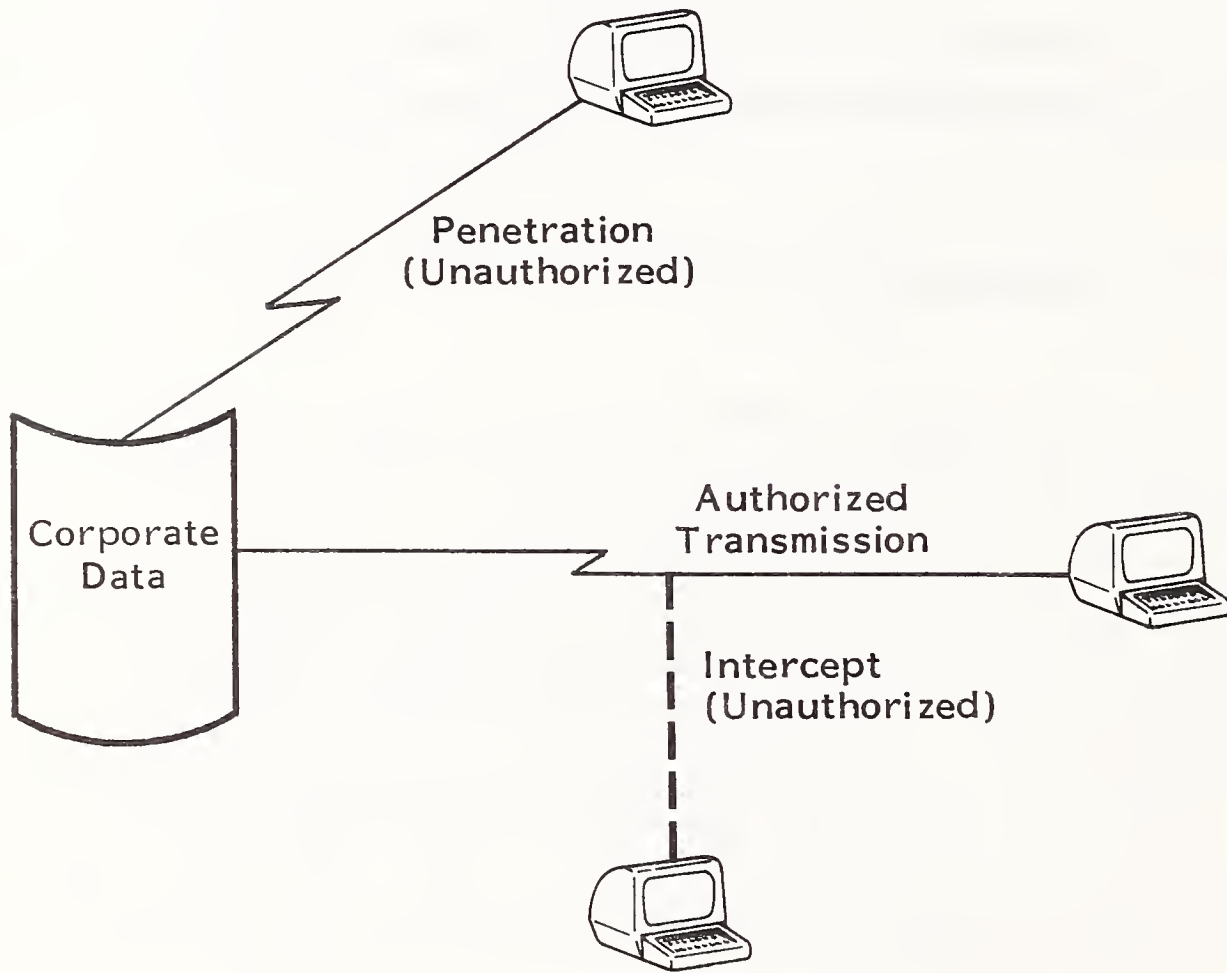
- Outsiders perpetrating a fraud usually take great pains to appear bona fide.
- Joy riders (or "hackers") often do not even have any close connection with a company, but choose their targets when opportunity presents itself (e.g., obtaining a single password).
- Traditionally, unauthorized data access has not been perceived as a very important data processing problem.
  - Most computer-stored data have been operational and of fairly low value.
  - Traditional computer-stored data were usually organized in such a way as to make it hard to navigate through to find the desired data.
  - Computer data have in the past been most valuable in printed form, after having been extracted and made usable. The advantage for a data thief is that the data are transportable and easily copied.
- The prevalence of on-line systems, especially those designed to be user friendly, is changing this.
  - Much more data are accessible by remote terminals.
  - Information center-type tools are making it easier to locate and collate specific pieces of data.
  - Increased use by non-IS staff combined with layered, complex software often make identification of unauthorized usage very difficult.
  - The very complexity of systems means that a great deal of attention is paid to making data accessible; this is inconsistent with security in many cases.



- Data files (including programs) can be penetrated. Data transmissions can be intercepted as well, as shown in Exhibit IV-1.
- Normally, interception would not be considered a high priority issue since one terminal's data would usually be of marginal interest to anyone.
  - However, the terminal traffic of, say, a firm's acquisition group might be very valuable information in the wrong hands.
  - An interception of multiplexed traffic can expose a wide selection of data to prying eyes.
  - By intercepting transmissions at one point, outsiders can learn how to penetrate the system elsewhere.
  - Companies installing their own satellite-based network may be exposing their entire telecommunications traffic to interception.
- Penetration is readily recognized as a problem. Files have been regularly penetrated by computer "hackers." Their efforts have shown that most computer systems (including that of at least one well-known timesharing firm) are easy to penetrate.
  - A walk through most terminal rooms will still find passwords taped to the CRT.
  - Once inside systems, master directories and other system control information are all too readily available.
    - The basic cause is that most data processors are generally concerned with making systems more, not less, accessible.
- Passwords can be made to work more effectively than they do at present.

EXHIBIT IV-1

UNAUTHORIZED DATA ACCESS



- People can be allowed to choose their own passwords; this will make it unnecessary to write them down.
- Users (and their supervisors) should receive a regular report of their recorded use on the system. Users can thus provide feedback on unauthorized use.
- Specific files should be accessible only to specific people and terminals.
- However, once the password system is breached (e.g., by obtaining the password of a systems programmer) it becomes difficult to bar an elite intruder.

## B. CONTROL MECHANISMS

- Traditionally, theft and fraud have been prevented and uncovered by the auditing process. Joy-riding vandalism is either obvious or becomes known after erratic system performance. Much theft, fraud, and joy riding are only discovered because of good luck or individual initiatives.
  - Auditors, both external and, to a large degree, internal are not really suited to identify computer-related fraud and theft.
    - Many do not have a deep knowledge of computer systems in general.
    - By the nature of their work they are usually not able to achieve a deep knowledge of individual functional areas or specific computer applications.
    - Most importantly, there is great controversy whether it is even part of the duties of an external auditor to aggressively seek out

theft and fraud. It would in any event greatly increase the cost of audits.

- IS technical staff is largely concerned with making computer systems more, rather than less, accessible. The "hacker" mentality is not present in most members of corporate IS staffs. The problem has not occurred often enough to have many people normally conscious of it.
  - Passwords, physical access control, and data set access control are the main line of defense. As indicated earlier, passwords are a weak barrier.
- Data set access control is accomplished by software packages that set conditions under which a system user can access the operating system and data sets (files and programs). Essentially, a directory is established which specifies which users (typically identified by password) can access which data sets and under what conditions.
  - The leading products are:
    - SECURE (Boole and Babbage).
    - ACF2 (Cambridge Systems).
    - SAC (EDS).
    - RACF (IBM).
  - These are useful products in that they compartmentalize the computer system with very small overhead. However, they have two limitations:
    - No product yet functions in a VM environment. This is a serious limitation, as VM is increasing in popularity, although it will presumably be met by a next-generation production.

- More seriously, these products are dependent on passwords to verify user identity (SECURE does not even use passwords but depends on JCL). Thus, the security chain is again dependent on that weak link, password control.

## C. POTENTIAL TECHNICAL SOLUTIONS

### I. SYSTEM PENETRATION

- The most critical need is to strengthen the user identification process. Passwords are adequate to control accidental or casual penetration, but not the determined penetrator.
- A solution to the password problem is to have a higher level of access tied to unchanging personal characteristics; i.e., biometrics.
  - Solutions that implement this kind of protection set up master files of digitally coded biometric measurements such as:
    - Fingerprints.
    - Hand geometry.
    - Signatures.
    - Voice prints.
- There are new products aimed at fingerprint, signature, and voice verification that represent potential price/performance breakthroughs. Hand-geometry identification (based on a scanned picture of an outstretched hand) does not appear to have the same level of precision as these newer products.

- In each case special terminals are used to collect the biometric information and forward it to a central computer, which matches the incoming metric to a stored copy.
  - The critical error rate for security purposes is the so-called Type II error (where an unauthorized person is incorrectly identified as authorized). All of these devices can produce an acceptable Type II error rate (about 1% or less). This assumes that they are used with an effective password system, establishing a double barrier.
  - There is a trade-off in that, by reducing the Type II rate, the Type I rate is usually increased (i.e., denying access to bona fide users). This is less of a problem where only internal staff is involved; however, exception procedures must not become a loophole for penetrators.
  - Even more important is guarding the central file of biometric data. Access to this file should have the highest level of security, e.g., requiring approved access by two people at the same time.
- The advantages and disadvantages of these biometric devices are shown in Exhibit IV-2.
  - The main disadvantage, common to all the devices, is that they have only been out of the R&D stage for a short time and, in at least one case, are not really on the market yet.
  - These are also small firms. Whether they have the resources to provide adequate support or even stay the course is not clear.
- However, each of these devices could play an important role in the IS security strategy.
  - An example of this is the tagging of critical files, directories, application programs, and parts of the operating system so that they would be

COMPARISON OF BIOMETRIC CONTROL SYSTEMS

BIOMETRIC CONTROL SYSTEM	ADVANTAGES	DISADVANTAGES
Fingerprint (Finger-matrix, White Plains, New York)	<ul style="list-style-type: none"> <li>● Very low error rate (0.03% Type II errors)</li> <li>● On market for 1½ years ("substantial" number of customers)</li> </ul>	<ul style="list-style-type: none"> <li>● Cost: \$5,000 for existing terminal upgrade, \$30,000 - 60,000 host modifications</li> <li>● Some social stigma (although probably fewer acceptance problems for internal use)</li> <li>● Damaged finger cannot be identified</li> <li>● May be confused with less accurate hand geometry product</li> </ul>
Voice Print (SecureTIP, New York, New York)	<ul style="list-style-type: none"> <li>● Low error rate (&lt; 1.0% Type II error)</li> <li>● Rental option (\$80/month)</li> <li>● Most user-friendly device</li> <li>● Can screen recordings</li> </ul>	<ul style="list-style-type: none"> <li>● Cost: \$6,500 purchase price for add-on box for terminal</li> <li>● Cannot use telephone lines, must have local box</li> <li>● Released October 1982; customers essentially Beta sites</li> <li>● Must overcome prejudice from previous vendor failures</li> </ul>
Signature Verification (Sycon, Santa Clara, California)	<ul style="list-style-type: none"> <li>● Acceptable error rate (about 1.5% Type II errors)</li> <li>● \$1,000 cost for upgrading existing terminals (\$500 in 1984?)</li> </ul>	<ul style="list-style-type: none"> <li>● Not released until mid-1983</li> <li>● Awkward to use in some environments</li> <li>● Some people cannot replicate signature</li> </ul>

NOTE: Product characteristics based on vendor-supplied information.

accessible only to a particular class of users, i.e., those with a biometric code (in addition to a password).

- Initially, the number of biometrically keyed files and users could be kept small. This would test the approach and also keep costs down. As more experience was gained and the devices' prices fell, more files could be biometrically tagged.
- Partly because of the small size and start-up position, these firms are largely focussing their efforts on what they perceive to be their best markets, that is:
  - Sensitive military and government applications.
  - Physical access security.
  - High-value, high-visibility dollar transactions.
- The "ordinary" data security market is one that may not receive high priority from these vendors for some time to come. IS departments that wish to evaluate these products may not only have to take the initiative but also be perceived as a good prospect for a significant amount of business for these firms to be able to devote sizable resources to an IS department's inquiries.

## 2. INTERCEPTION

- Interception can be dealt with in several ways, by:
  - Cryptography.
  - Fiber optics transmission media.
  - Decentralized data processor.
- None of these approaches is a panacea, however.



a. Cryptography

- Cryptography is obviously of critical importance when sending very important messages; e.g., those associated with national security.
  - Enciphered data is not appropriate for the vast majority of commercial data traffic. It is overkill with significant computer processing and control overhead.
  - For organizations that do produce some sensitive traffic (e.g., banks), enciphered communications are an option. However, many governments, especially in Europe, have become very nervous over trans-border, enciphered data flows.
  - Much has been made in professional publications about the "key" in the cryptographic standard not being large enough to prevent government agencies cracking the code. In the commercial world this is usually not a significant impediment to use.
- Cryptographic solutions can produce an unwarranted belief in the level of interception protection. Cipher keys are, in principle, identical to passwords. Once the key is in possession of an unauthorized person, the enciphered message is easily translated. Changing keys is no solution if the outsider has access to the key location. Key security is critical to a secure enciphered network.

b. Fiber Optics

- A fiber optic transmission medium is virtually impossible to tap. However, there are no all-fiber optics circuits in place yet from one user to another. It will not be technically or economically attractive for corporations to install short distance fiber optic networks merely for security purposes.
  - This will be a more common solution in the late 1980s.

c. Decentralized Data Processing

- Decentralized data processing, at its simplest and most effective, means downloading a sensitive file onto a floppy disk and transporting it to a personal computer at the location that would be performing the analysis. Data security then becomes physical security (i.e., locking up the floppy disk along with other workpapers).
  - Problems will arise in the future, however, as personal computers are increasingly linked into networks - one of whose chief rationales will be to share data!
  - For some time to come, personal computers will incorporate minimal security features. The current trends in the major personal computer operating systems (CP/M, MS-DOS) are to make data and program sharing easier; UNIX, the rising personal computer favorite, has always been deficient from a security standpoint.
  - Security in a personal computer environment can only be assured in a single user, single machine setting.
- Distributed data processing (i.e., local processors such as 4300s or 8100s sharing data files and processing loads with a central processor) offer some security advantages but also present serious problems.
  - On the positive side, local processors may be able to take up the slack in the event of a central processor failure. The system must have been designed with this as a major criterion for it to work, however.
  - Typically, key functions and files remain at the central location. In the absence of the central processor, the DDP network is like a snake with its head cut off: the body continues to move, but eventually everything comes to a stop.

- The chief security problems arise from the fact that the data is dispersed but still potentially accessible from many points in the system. The complexity and physical dispersion of the network makes it difficult to establish, monitor, or enforce data security safeguards.

#### D. SUMMARY

- Potential technical solutions discussed above do hold promise of alleviating some problems. However, technical solutions must be aimed at the areas of greatest potential loss and vulnerability. Present methods are not satisfactory for making this kind of decision. Too much is dependent on individual judgment or hunches.
  - It is necessary to reintroduce the human element into problems that are, after all, primarily human in origin.

#### E. A COUNTER-PENETRATION PROGRAM

- Technological techniques to guard files suffer from the Maginot Line Syndrome: no matter how impressive the defense, it is static; intruders can decide exactly where and when to strike, seeking out lightly defended areas.
  - What is needed is a means to anticipate the areas that might be attacked, strengthen them, and perhaps, catch the intruder in the act.
- To do this, it is necessary to duplicate, at least to a degree, the reasoning of potential intruders and block the gaps that have been identified.
  - What would be the best way to commit a fraud?

- How could one illegally enter a system and, once there, gain control?
- Slightly different techniques are used to deal with the theft/fraud and joy-riding areas:
  - An interdepartmental "threat team," as reported by Brandt Allen of the University of Virginia, should be used to forestall theft and fraud.
  - A small group of IS technicians can be used to create a "war game" environment.
- Threat Teams: This is a group of operations-oriented staff assembled from both IS and user areas to assess a specific area; e.g., accounts receivable, accounts payable/receiving, inventory control, etc.
  - Initially, the group discusses the weak points of the system involved. Members are invited to hypothesize how an individual might tamper with the entire process in order to subvert it. Groups are generally quite creative and pragmatic in their assessments.
    - The group estimates how easy it would be to do, how long it could be done for, and the damage that could be done.
    - Finally, the group devises a plan to change the system to prevent the abuse in the future.
  - Although the threat team approach is in its infancy, it has produced good results where it has been used. Guidelines for increased success are:
    - Not including a supervisor and a subordinate on the same team.

- The leader should have had prior experience in small group leadership; ideally, experience in leading threat team assessments.
  - Team members should not know in advance the purpose of the meeting.
  - Work should be accomplished in two or three meetings.
- War Games: The members of this group would come only from the IS technical staff. Membership should be part time and temporary as a means of gaining fresh ideas and for security purposes.
  - For security purposes, there should always be at least two members working on a problem and detailed documentation should be kept.
    - As with the threat teams, there should be specific assignments; e.g., "with only a valid password could I crash the system?"
    - For obvious reasons, live tests on the system should be performed at noncritical times or on a duplicate version of the system.
  - This war gaming capability is already offered by some consultants who adopt the role of an outside penetrator and attempt to enter the system. This source is certainly a viable alternative, especially if internal staff does not have the war gaming attitude or it is thought undesirable to have employees subvert the system. However, there are definite advantages to using internal staff.
    - Staff will become more knowledgeable about the system.
    - They may be better placed to consider how fellow employees could enter forbidden parts of the system.

- War gaming is not a one-time effort but should be performed continuously.
- Internal staff will add to their own knowledge of the system and may be better able to prevent or recover from system crashes caused by bona fide accidents.

## V ASSESSING AND DEALING WITH RISK

### A. APPROXIMATE RISK ANALYSIS

- The preceding discussion of physical threats and unauthorized file access indicates that the range of potential problems and possible solutions is very large. So large, in fact, that no organization's resources are sufficient to provide 100% security.
  - What is needed is a methodology to decide where to apply resources so that the risk of damage will be minimized.
  - Risk analysis is the means of comparing costs and benefits.
- At its simplest, risk analysis is the calculation of the potential loss if a particular event occurs, such as a fire in a certain class of building or the death of a person with certain characteristics. It is the principle underlying the insurance industry.
- Ideally, all risks could be evaluated by means of a formula which would place a loss value on a risk by calculating the probability that a particular event would occur (e.g., that computer power will fail for a six-hour period in the next year), multiplied by the dollar amount of the consequent loss.

- This is the general approach taken by the PANRISK package marketed until recently by Pansophic Systems.
- There are two problems with this theoretical approach as applied to computer security:
  - There is inadequate data with which to calculate with precision some key probabilities, such as the availability of a commercial disaster center if a client's computer center were destroyed.
  - Even more important, it is very difficult to quantify many types of computer-related losses. For example, if an order entry system is inoperable for four hours, how many orders will be permanently lost? If the outage were two hours or eight hours, would the resulting losses be half as great or twice as great?
- These difficulties have made the application of conventional risk analysis difficult in the computer security area. In addition, many IS managers and user personnel would feel uncomfortable using such a mechanical methodology, even if it were more accurate.
  - Some very important effects of a computer system failure may be virtually impossible to quantify in any meaningful way. Examples of these kinds of effects include:
    - Decreased efficiency in carrying out (internal) organizational functions.
    - Lower quality customer service.
    - A slump in production.
    - Threatened organizational viability or existence.



- Fortunately, the recent mathematical formulation of the theory of "fuzzy sets," provides an intellectual foundation for performing an approximate analysis, in situations such as risk analysis, where precise quantitative analyses are not the norm.
  - However, some experts believe that it is not necessary to apply the theory of fuzzy sets itself, but to use the idea of approximating risks.
  - That is, rather than using values of "10" and "100," one might instead say "low" and "very high." It is not necessary to think of precise numbers, or any quantifiable value at all, when using such terms.
- Using this kind of approach, it is possible to arrive at approximate risk analysis, using words to represent a scale from very low to very high. One of the advantages of using words on the scale, rather than numbers, is that numbers can imply a precision that does not, in fact, exist.
- Exhibit V-1 provides an example of using words for a computer-related risk analysis to construct a severity scale to classify the kinds of disruptive situations previously described. Note that the various effects have been consolidated into three groups:
  - Permanent revenue loss is that which will almost certainly not be recoverable. The amounts in the exhibit may be adjusted to be consistent with the size and outlook of the organization to which they would be applied.
  - Losses arising from disrupted organizational functions will depend on how efficiently various parts of the organization perform after different types of computer system damage.
  - Basic mission losses are those which affect how well the corporation is able to continue to supply the products and/or services that are its rationale for existing.

EXHIBIT V-1

SEVERITY SCALES FOR EFFECTS OF DISRUPTIVE SITUATIONS

SEVERITY SCALE	REVENUE LOSS (permanent)	EFFECT ON ORGANIZATIONAL FUNCTIONS	EFFECT ON BASIC MISSION
Very Low	< \$100,000	Scattered Loss of Efficiency	Few Effects on Customers/Production
Low	\$100,000-500,000	Widespread Loss of Efficiency	Service/Production Affected, but Adequate Levels Maintained
Medium	\$500,000 - \$1 million	Some Individuals Unable to Perform Their Duties Adequately	Significant Additional Expense Incurred to Maintain Service/Production Levels; <u>or</u> Adequate Service/Production Levels Not Maintained
High	\$1-5 million	Many Individuals or Some Departments Unable to Perform Their Duties Adequately	Viability of Organization Threatened
Very High	> \$5 million	Many Departments Unable to Perform Their Duties Adequately	Organization is no Longer Viable

- Assessments can be made for key computer applications that would be disrupted by a computer system malfunction.
  - Exhibit V-2 provides a conceptual worksheet for supplying the inputs for an approximate risk analysis related to physical threats.
  - The analysis itself could not and should not be a mechanistic averaging of the risk factors across various applications. To take an extreme case:
    - If all applications except one show very low effects arising from a long outage but the effect on the remaining application threatens the organization's viability, vigorous measures would have to be taken.
- A "Fuzzy Metrics" prototype package is now under development by Information Policy, Inc. (Washington, DC). This would be of assistance in organizing the data obtained when performing approximate risk analyses.
  - However, approximate risk analysis can be profitably undertaken in a manual setting. The value is in the analysis, not in the mechanics.
- Risk analysis may also show that the effects of a particular computer problem may not be a straight line relationship. Exhibit V-3 shows the different effects that computer outages can have on different types of applications.
  - Estimated profiles should be constructed for all important applications.
- The previous discussion of risk analysis purposely used computer outages as a vehicle: their incidence can be measured, or at least reasonably assumed, and it is fairly straightforward to estimate their effects. The approximations are in many cases for values that can almost be quantified.

EXHIBIT V-2

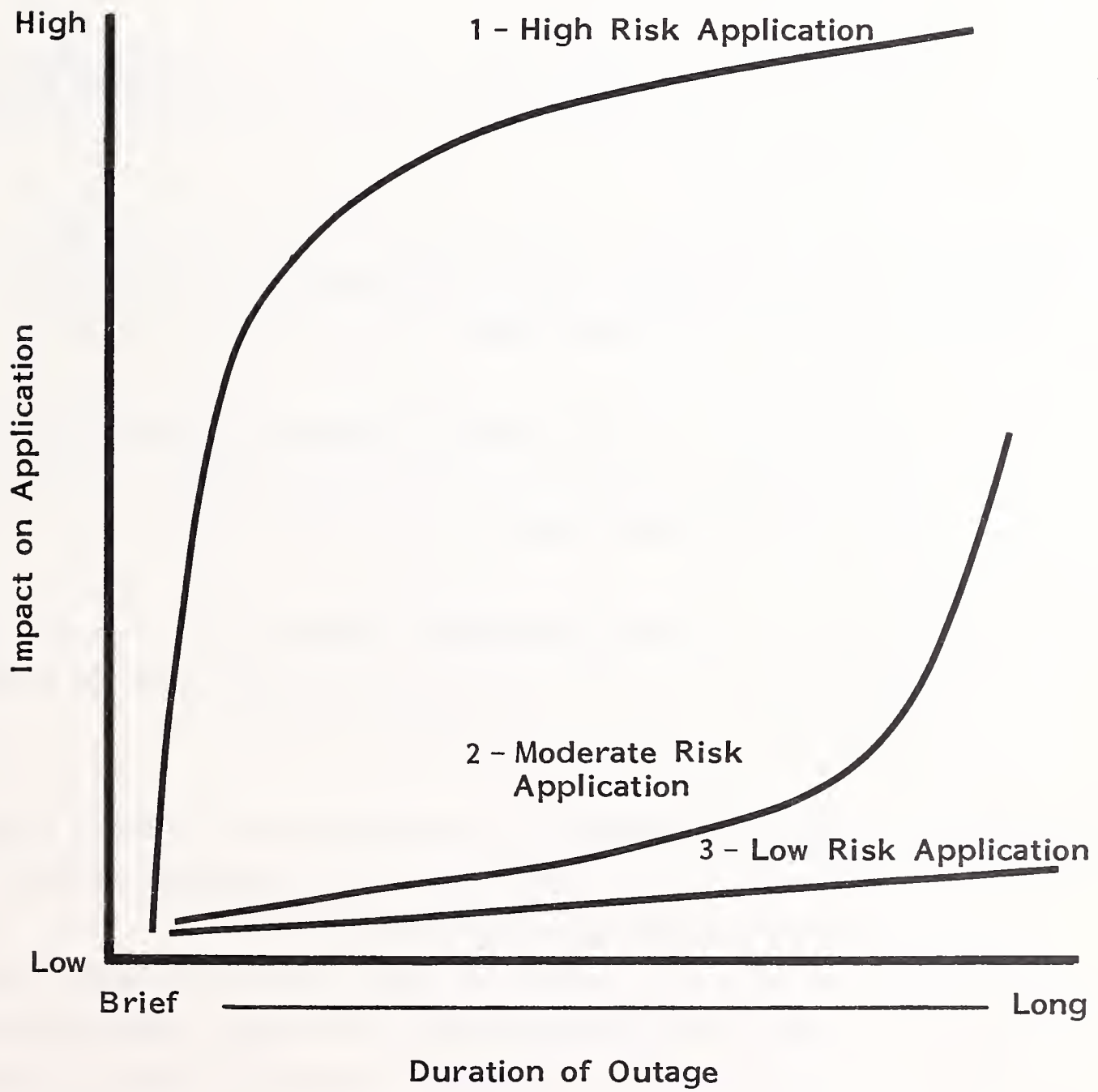
EFFECTS OF DISRUPTIVE SITUATIONS (WORKSHEET)

Disruptive Situation	Number Per Year*		Extent of Effects (For Major Applications)														
			Application A			Application B			Application C			Application "N"					
			Rev. Loss	Org. Func.	Mission	Rev. Loss	Org. Func.	Mission	Rev. Loss	Org. Func.	Mission	Rev. Loss	Org. Func.	Mission			
Line Disturbance (noise, transients)	Power Related	Other															
Momentary Outages (< 1 second)																	
Brief Outage (1 second-15 minutes)																	
Long Outage (15 min.-several hours)																	
Very Long Outage (> several hours)																	
Permanent Outage																	

\* Quantify or express on scale from very low to very high

EXHIBIT V-3

IMPACT OF A COMPUTER OUTAGE ON  
DIFFERENT TYPES OF APPLICATIONS



- Analyzing the risk involved to data files and program code is much more difficult and inexact than evaluating physical threats.
  - The incidence of theft, fraud, and joy riding is unknown and probably unknowable.
  - There are very few packages of products or services to deal with the problems of data threats.
  - There is a much greater range in the amount of loss possible, since a transient in a check print file or an audacious fraud can lead to losses in the millions.
  
- However, counter-penetration efforts can greatly assist in defining the overall problem as well as providing solutions.
  - The counter-penetration groups will be able to identify the major problem areas. In many cases, they will also be able to estimate levels of dollar and nondollar risks.
  - Frequently the counter-penetration group can make its own implicit judgment about whether a threat is important enough to warrant full consideration.
    - It is important that the reasoning be made explicit so that data threats to a particular organization be better understood.
    - It is also important to take note of the data threats not considered important enough to pursue. This will enable an incidence rate of important data threats to be constructed. It will also allow for the differing characteristics of major and minor data threats to be identified.

- Exhibit V-4 provides a worksheet for data threats similar to the one for physical threats.
  - The threats, of course, cannot be categorized in advance.
  - The effects of the threats will also be more difficult to put into uniform groups.

## B. INSURANCE

- Required insurance coverage should be one of the direct outcomes of a successful risk analysis. Even if precise loss levels cannot be established in all cases, at least the range of required coverage should be clear.
- Any significant security incident can result in monetary loss.
  - The loss can be a direct result of the incident itself, such as:
    - Computer hardware replacement.
    - Facility replacement.
    - Overtime, travel, etc. for restarting operations at another site.
    - Fraud and theft loss from computer system penetration.
  - Other losses can occur as an indirect result of a computer-related incident (typically as a result of inability to use the computer system), such as:
    - Lost revenue.





- Interest on increased working capital.
  - Additional expenses of alternate noncomputerized systems.
- Insurance can compensate for some or all of these losses (except, in some insurance policies, for internal fraud). IS, working with its corporate insurance or risk management specialists, should ascertain how many and what portion of potential losses are covered by existing policies.
  - The major applicable coverages would be property damage and business interruption policies; increasingly, insurers are offering comprehensive policies against most risks.
  - This analysis may be complicated by the fact that general policies are not written with computer-related loss specifically in mind.
  - Where a company is self-insured, in whole or in part, then the terms of reinsurance agreements are controlling.
- This analysis of existing coverage will be divided into three categories.
  - Threats definitely covered and the amount of coverage.
  - Threats covered partially or ambiguously.
  - Threats not covered.
- As a guiding principle, IS should not be overly concerned with having coverage against minor cost areas (e.g., coverage from a brief stoppage). Large deductibles make sense from a business standpoint. Most companies have established policies on deductible levels, whether valuation is at depreciated or replacement cost, etc.

- However, after excluding minor cost areas and deductibles, IS may find that considerable potential losses are not covered by existing insurance. This will not be surprising since standard policies were developed before computer systems became important.
  
- Several insurance companies now write policies specifically aimed at computer-related losses.
  - Companies writing such policies include American International, Fireman's Fund, Hartford, and St. Paul. An exceptional insurance broker can help determine which policy (if any) is most suitable for a particular organization.
  
  - Special care must be taken that using specialized computer loss policies does not result in specialized duplicate coverage.

**MANAGEMENT PROGRAMS:** Designed for clients with a continuing need for information about a range of subjects in a given area.

- Management Planning Program in Information Systems - Provides managers of large computer/communications facilities with timely and accurate information on developments which affect today's decisions and plans for the future.
- Management Planning Program for the Information Services Industry - Provides market forecasts and business information to software and processing services companies to support planning and product decisions.
- Company Analysis and Monitoring Program for the Information Services Industry - Provides immediate access to detailed information on over 3,000 companies offering turnkey systems, software and processing services in the U.S. and Canada.
- Management Planning Program in Field Service - Provides senior field service managers in the U.S. and in Europe with basic information and data to support their planning and operational decisions.
- On-Target Marketing - A practical, "how-to-do-it" methodology for more effective marketing problem solving and planning delivered to clients via workshops and/or consulting services.

**MULTICLIENT STUDIES:** Research shared by a group of sponsors on topics for which there is a need for in-depth "one-time" information and analysis. A multiclient study typically has a budget of over \$200,000, yet the cost to an individual client is usually less than \$30,000. Recent studies specified by clients include:

- Selling Personal Computers to Large Corporations
- Improving the Productivity of Systems and Software Implementation
- User Communication Networks and Needs
- Improving the Productivity of Engineering and Manufacturing Using CAD/CAM

**CUSTOM STUDIES:** Custom studies are sponsored by a single client on a proprietary basis and are used to answer specific questions or to address unique problems. Fees are a function of the extent of the research work. Examples of recent assignments include:

- Organizing for Effective Software Development
- Investigation of TSO and Comparable Systems
- Corporate Plan for Utilizing CAD/CAM
- 1981 ADAPSO Survey of the Computer Services Industry
- Analysis of Business Services for a Major Financial Institution
- Study of the Specialty Terminal Market
- Evaluate Information Industry Innovations

# ABOUT INPUT

INPUT provides planning information, analysis, and recommendations to managers and executives in the information processing industries. Through market research, technology forecasting, and competitive analysis, INPUT supports client management in making informed decisions. Continuing services are provided to users and vendors of computers, communications, and office products and services.

The company carries out continuous and in-depth research. Working closely with clients on important issues, INPUT's staff members analyze and interpret the research data, then develop recommendations and innovative ideas to meet clients'

needs. Clients receive reports, presentations, access to data on which analyses are based, and continuous consulting.

Many of INPUT's professional staff members have nearly 20 years' experience in their areas of specialization. Most have held senior management positions in operations, marketing, or planning. This expertise enables INPUT to supply practical solutions to complex business problems.

Formed in 1974, INPUT has become a leading international consulting firm. Clients include over 100 of the world's largest and most technically advanced companies.

---

## OFFICES

### Headquarters

P.O. Box 50630  
Palo Alto, California 94303  
(415) 493-1600  
Telex 171407

### Dallas

Campbell Center II  
8150 N. Central Expressway  
Dallas, Texas 75206  
(214) 691-8565

### New York

Park 80 Plaza West-1  
Saddle Brook, New Jersey 07662  
(201) 368-9471

### United Kingdom

INPUT, Ltd.  
Airwork House (4th Floor)  
35 Piccadilly  
London, W 1.  
England  
01-439-4442  
Telex 269776

## AFFILIATES

### Australia

Infocom Australia  
Highland Centre, 7-9 Merriwa St.,  
P.O. Box 110,  
Gordon N.S.W. 2072  
(02) 498-8199  
Telex AA 24434

### Italy

PGP Sistema SRL  
20127 Milano  
Via Soperga 36  
Italy  
Milan 284-2850

### Japan

Overseas Data Service Company, Ltd.  
Shugetsu Building  
No 12 - 7 Kita Aoyama  
3-Chome Minato-ku  
Tokyo, 107  
Japan  
(03) 400-7090  
Telex J26487

### Sweden

P.O. Persson Konsult AB  
Box 221 14  
Hantverkargatan 7  
104 22 Stockholm  
Sweden  
08-52 07 20

**INPUT  
MANAGEMENT  
PLANNING PROGRAM  
IN  
INFORMATION SYSTEMS**

VENDOR WATCH REPORT

**SOFTWARE MAINTENANCE:  
THE UNINVITED GUEST**

**NOVEMBER 1982**

# MANAGEMENT PLANNING PROGRAM IN INFORMATION SYSTEMS

**OBJECTIVE:** To provide managers of large computer and communications systems with timely and accurate information on developments which affect today's decisions and plans for the future.

**DESCRIPTION:** Clients of this program receive the following services each year:

- Impact/Planning Support Studies - In-depth reports dealing with the impact on users of projected managerial, personnel, and technological developments over the next five years.
- Technology and Management Issue Briefs - Analyses of the probable moves of major computer/communications vendors in operating systems, data base/data communications software, mainframes, value added networks, and other marketing services.
- Residual Values - The residual values of major mainframes.
- Annual Long-Term Forecasts - Long-term forecasts of both short- and long-term trends in the industry. Managers by major industry are invited to participate in the forecasts during the second half of the year.
- Conferences - Conferences at a convenient location in the area.
- Inquiry Services - Inquiry services as-needed.

## RESEARCH METHODS

- Research conducted by experienced researchers.
- Research conducted by university professors.
- Conclusions based on the judgement of INPUT's research staff.
- Professional experience in the field of senior management.

For more information on this report, please call or write:

INPUT  
Park 80 Plaza West-1  
Saddle Brook, NJ 07662  
(201) 368-9471

or

INPUT  
P.O. Box 50630  
Palo Alto, CA 94303  
(415) 493-1600 Telex 171407

# INPUT

## INFORMATION SYSTEMS PROGRAM

VENDOR WATCH REPORT

SOFTWARE MAINTENANCE:

THE UNINVITED GUEST

NOVEMBER 1982





# SOFTWARE MAINTENANCE: THE UNINVITED GUEST

## CONTENTS

	<u>Page</u>
I MANAGEMENT SUMMARY AND RECOMMENDATIONS .....	1
A. Summary	1
B. Recommendations	4
II CURRENT MAINTENANCE ISSUES .....	7
A. What Is Software Maintenance?	7
B. Overview Of Issues	10
C. The Characteristics Of Maintenance	10
D. Maintenance Elimination	18
III MAINTENANCE INITIATIVES .....	25
A. Technical Initiatives	25
B. Administrative Control Initiatives	26
C. Organizational Initiatives	27
1. The Location Of The Maintenance Function	27
2. User Communications	28
D. Personnel And Management Initiatives	36
E. Conclusion	37

# SOFTWARE MAINTENANCE: THE UNINVITED GUEST

## EXHIBITS

		<u>Page</u>
I	-1 Customer Satisfaction With Vendor Software Maintenance	2
	-2 In-House Maintenance Requirements For Software Packages	5
II	-1 Functions Included In Vendor Software Maintenance	8
	-2 General Hardware/Software Cost Trends	11
	-3 Software Development - Maintenance Trade-Offs	12
	-4 New Program Development Versus Maintenance - 1981-1983	13
	-5 Software Modification Costs In Different Development Stages	14
	-6 Components Of Software Maintenance	16
	-7 Capacity Limitation Effects On Maintenance Costs	17
	-8 Comparison Of Maintenance And New Development	19
	-9 Can Maintenance Be Eliminated?	22
	-10 Maintenance Alternatives	23
III	-1 Alternate Maintenance Organizations	29
	-2 Advantages And Disadvantages Of Alternate Maintenance Organizations	30
	-3 A Software Support Center	32
	-4 Maintenance Communications In A Software Vendor Environment	34
	-5 Frequency Of Maintenance Activities	35

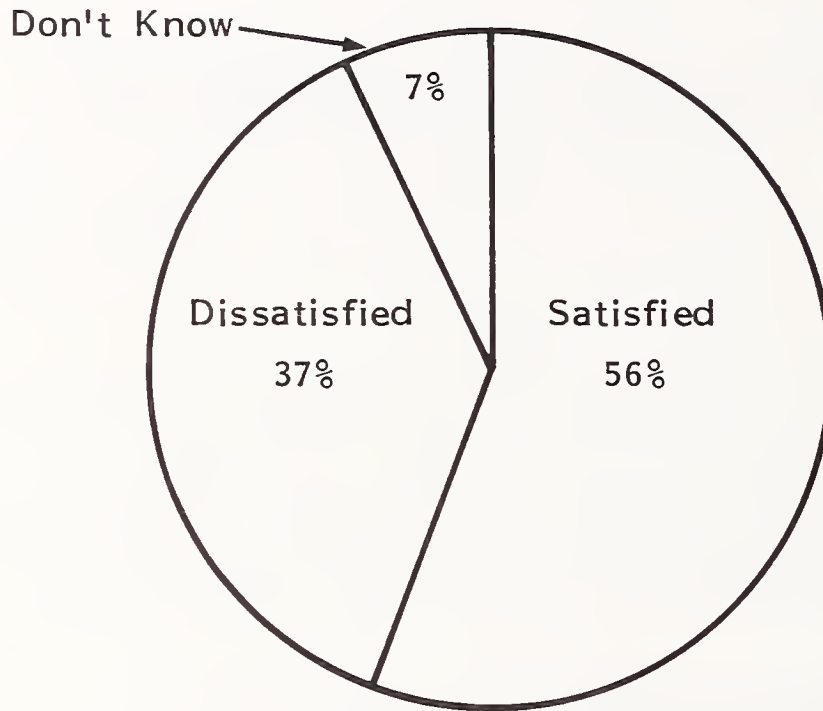
## I MANAGEMENT SUMMARY AND RECOMMENDATIONS

### A. SUMMARY

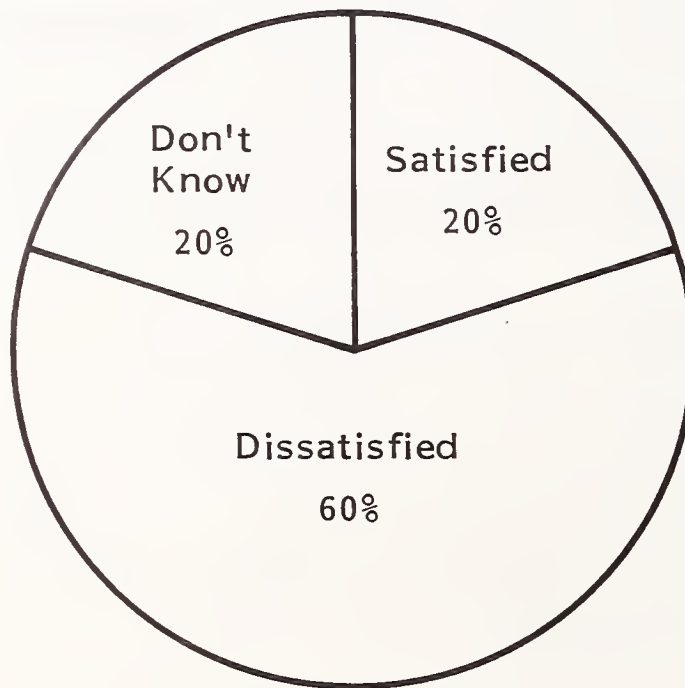
- Maintenance activities play a much larger role in the perceived success or failure of IS activities than most IS organizations realize.
  - Consider four facts:
    - For most IS organizations, maintenance consumes about half of the in-house software (i.e., programmer and analyst) resources.
    - Virtually all the systems users come in contact with are operational, hence, in maintenance status.
    - Almost all programming work requests from users are for maintenance activities (including enhancements). Sometimes, of course, only a new system can get the user (and IS) out of a particular dead end, but it is a maintenance problem until the painful and usually expensive decision is made to implement a new system.
    - Even software companies are faced with a similar problem with their customers, as shown in Exhibit I-1.

EXHIBIT 1-1

CUSTOMER SATISFACTION WITH VENDOR SOFTWARE MAINTENANCE



SOFTWARE COMPANIES



HARDWARE COMPANIES

Percent of Companies Perceiving  
Their Customers as Satisfied  
or Dissatisfied

SOURCE: Input Survey

- In spite of the importance and visibility of maintenance functions, maintenance is a stepchild in most IS departments.
  - New system development receives the lion's share of management attention.
  - Maintenance is too often a question of fire fighting.
  - There is usually no maintenance staffing philosophy: maintenance is more often than not staffed by trainees, marginal performers, and those exiled to Siberia.
  - The only career path open to superior performers is out of maintenance.
- If anything, maintenance is more demanding than new development, but the tools and management support provided are rarely adequate.
- Some authorities believe that the amount of maintenance needed will decrease.
- They see this occurring because:
  - User-developed systems will expand in number and importance. The personal computer explosion is one aspect of this; the Information Center is another.
  - Software packages will penetrate even more deeply into most organizations. Newer packages will be more flexible and easier to use.
  - Software will be of higher quality as software productivity tools are more widely used.
- There is little doubt that these three trends are all occurring and will have many beneficial effects. However, IS maintenance tasks and associated

resources required will not diminish appreciably and will probably continue to grow.

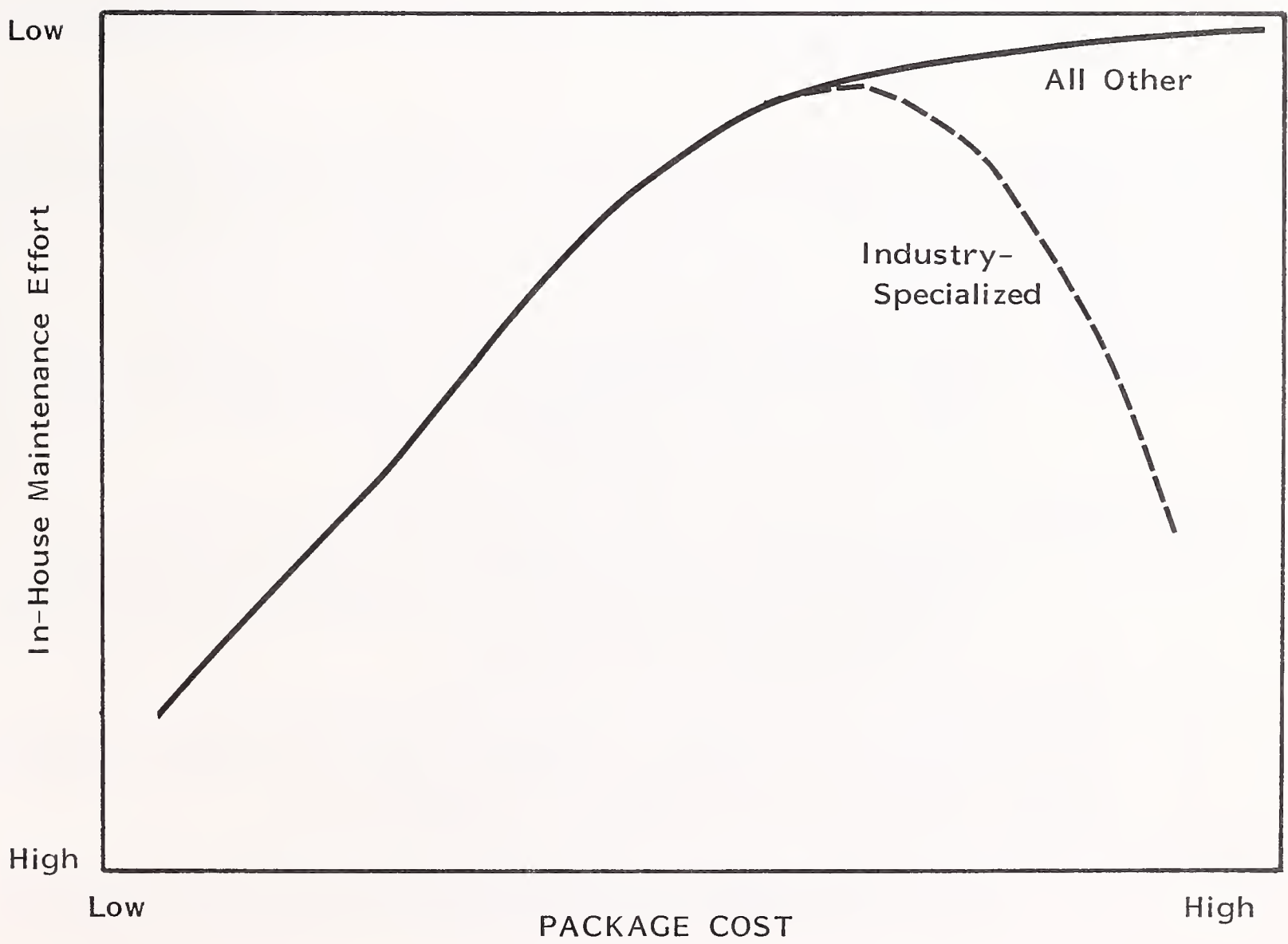
- User-developed systems largely serve needs that are considered low priority in IS prioritization processes. Consequently, the core development and maintenance workload is not going to go away. Equally important, even user-developed systems have to be maintained by someone. Some software packages do relieve IS departments of much, if not all, maintenance burdens. However, there are key exceptions to this.
  - Very inexpensive packages, most notably those for personal computers, cannot provide much in the way of support or modifications.
  - Similar problems exist on the other end of the spectrum. Large, industry-oriented packages must often make compromises that result in packages that are both hard to install and hard to maintain. Consequently, some organizations (e.g., the insurance or banking industries) purchase large software systems to use only as a framework. After tailoring, these will require in-house maintenance as much as a custom-developed system. Exhibit I-2 illustrates these relationships.

## **B. RECOMMENDATIONS**

- The most important change required in most organizations is for IS management to make maintenance one of its priorities. This will give maintenance credibility and self-respect.

EXHIBIT I-2

IN-HOUSE MAINTENANCE REQUIREMENTS FOR SOFTWARE PACKAGES



- Large IS departments should separate maintenance and development organizationally. This is a key step for building maintenance, morale, career paths, and tools.
- Organizations would be unwise to assume that there is a distinctive maintenance personality. Maintenance tasks require high skills plus the frequent need to work alone in an unstructured environment.
- Good development techniques will pay off in easier maintenance later on. It takes tough-minded management to make this kind of up-front investment in time and resources, however.
- There are no maintenance technologies and tools analogous to those offered for new development work (e.g., structured design, Jackson, Warier-Orr, Gane & Sarson, SADT).
  - In the short-term, maintenance must be taught by apprenticeship. The strategy is to identify those that are good at both maintenance and teaching, and let them reproduce themselves.
  - In the long-term, tools will emerge (especially in connection with the Ada support environment now being constructed). Stay informed about them, and implement them cautiously.
- The maintenance process should be monitored both for immediate management purposes and to create a maintenance data base that will:
  - Identify differential rates of maintenance success between individuals.
  - Identify problem-prone systems/departments.
  - Test the effectiveness of new approaches to maintenance.
- IS departments should benefit from software vendor experience and consider creating a software support center.



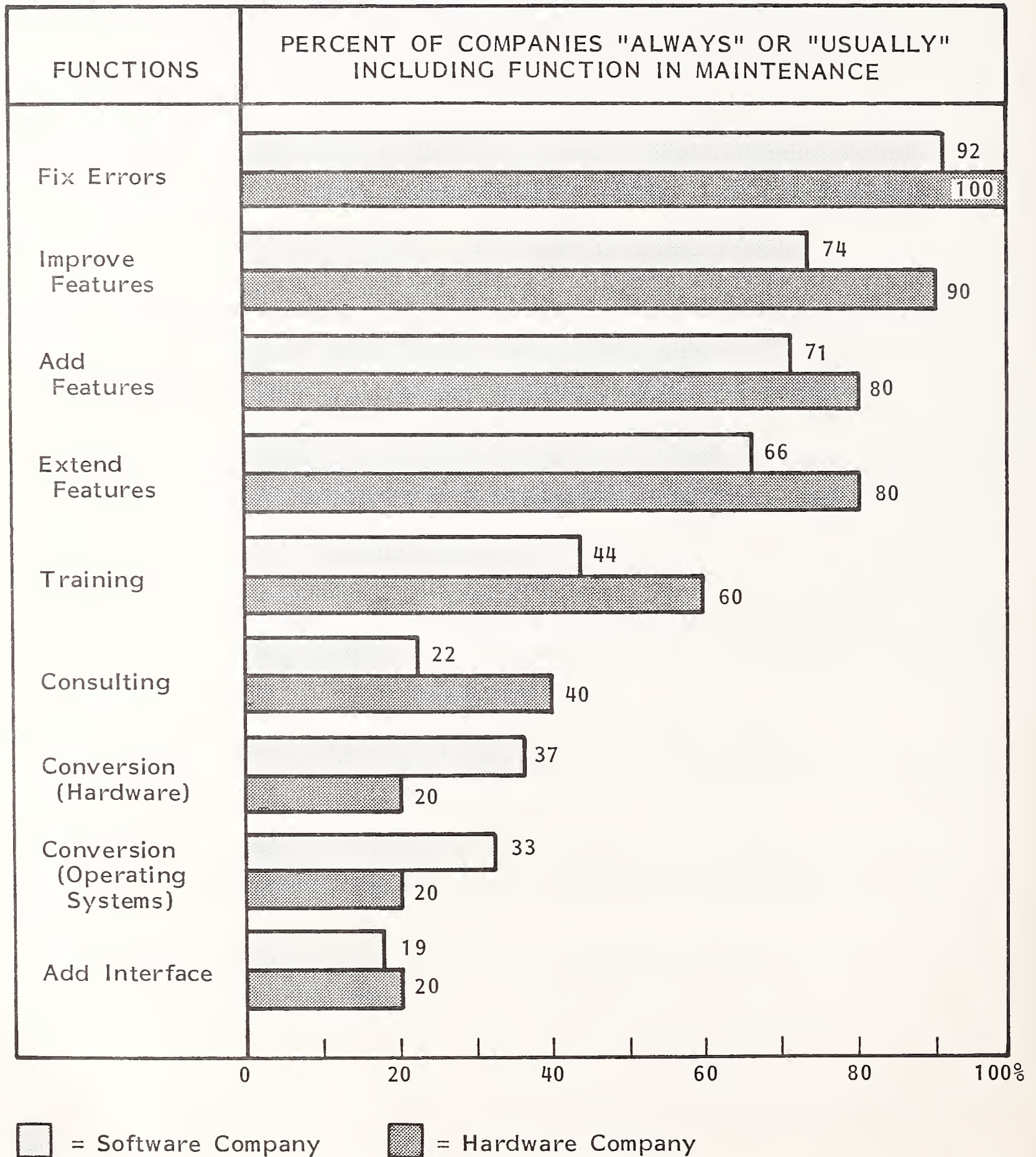
## II CURRENT MAINTENANCE ISSUES

### A. WHAT IS SOFTWARE MAINTENANCE?

- "Software maintenance" does not have a commonly accepted definition in either the user or vendor community. Exhibit II-1 shows the areas of agreement and disagreement between software and hardware vendors. It is useful for IS departments to examine vendor practices in this area since they generally have more mature maintenance organizations and more comprehensive maintenance philosophies.
- Virtually all vendors agree that fixing software errors is included in software maintenance. It is interesting that a few software vendors do not see even this as part of their responsibilities.
  - Most vendors also see improving, adding, and extending features as part of software maintenance.
  - Software vendors are much less likely than hardware vendors to include training and consulting in maintenance.
  - Supplying conversion and interface assistance are seen by only a minority of vendors as being part of maintenance.

EXHIBIT II-1

FUNCTIONS INCLUDED IN VENDOR SOFTWARE MAINTENANCE



SOURCE: INPUT Survey

- Generally, software vendors include fewer activities in maintenance than hardware vendors, except for conversions.
  - Hardware vendors take a more inclusive view of maintenance because they are used to taking a more comprehensive view of customers' needs; in addition, a bundled services attitude in many cases has survived unbundling.
  - The exception for conversions points up the different roles of hardware and software companies. Hardware companies will only consider conversions within their own hardware line while software companies will make any conversions that are economically attractive.
- Hardware vendors have not changed their definition of maintenance in the past three years. However, 30% of the software vendors reported doing so to adapt to new markets and product areas.
- Both hardware vendors (60%) and software vendors (44%) expect to be making changes in the activities included in software maintenance. Both types of vendor will try to reduce the extent of services and activities included in maintenance in order to reduce costs.
- Fewer than half the vendors view training and consulting as activities normally part of software maintenance.
- There is consequently a built-in tension between what vendors see as software maintenance and actual needs for software maintenance.

## B. OVERVIEW OF ISSUES

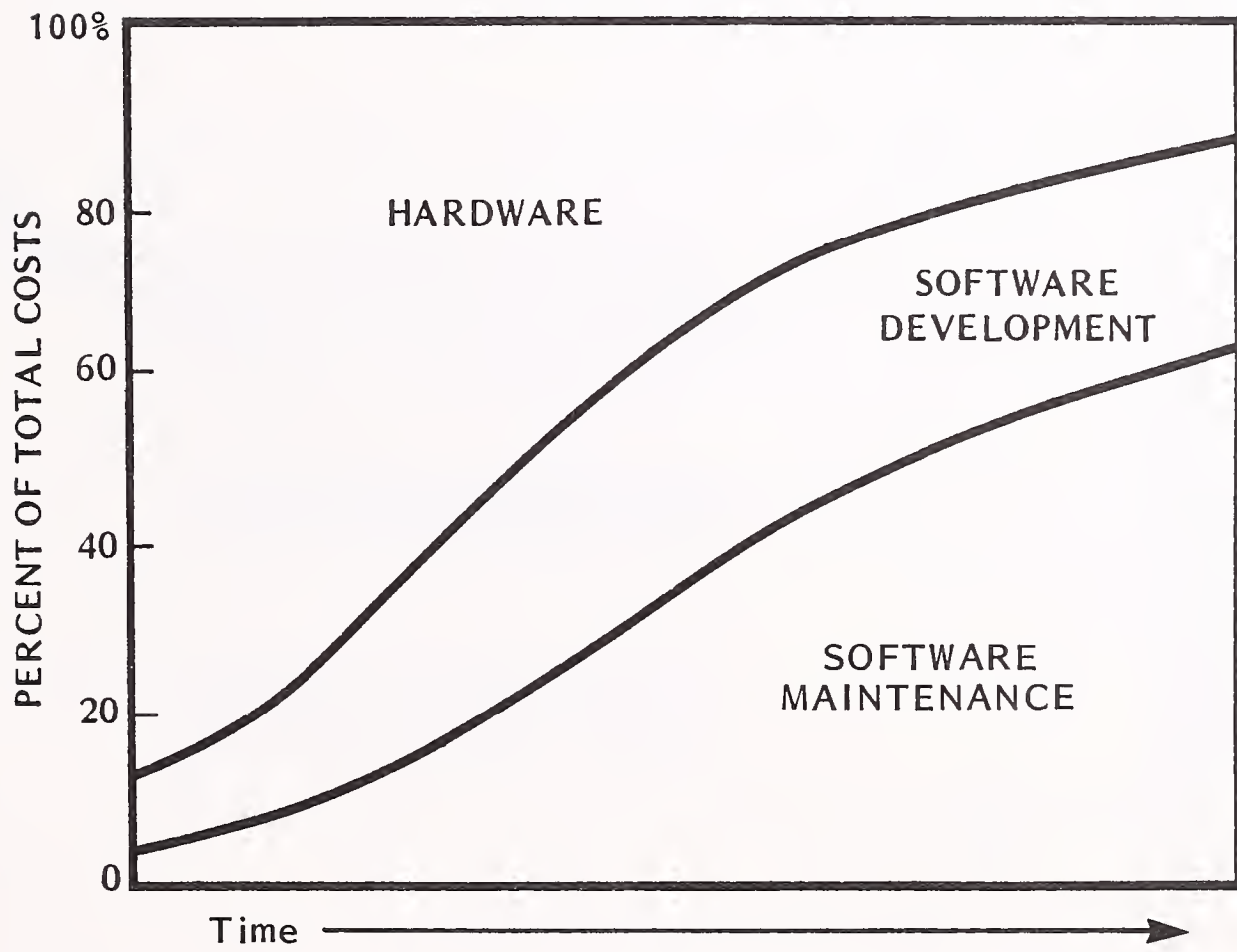
- It is a well-known fact that hardware costs within total systems are falling while software costs are rising. What is not always recognized is that software maintenance costs have been rising for some time, as shown in Exhibit II-2.
- Exhibit II-2 purposely has a time scale left off because, at least as far as software is concerned, the cost ratios depend on the age of the system, as shown in Exhibit II-3.
  - For most systems development costs are only 30% to 40% of total life cycle costs.
  - Looking at it another way, at any particular point in time the typical IS department is spending about half of its programming and systems resources on software maintenance, as shown in Exhibit II-4. In addition, a considerable amount of "new" development consists of enhancing existing systems.
- These facts are usually unrecognized, if not intellectually, then by actions. Far and away the most attention and planning is focused on new systems, tools for building new systems, and people to staff new systems. This may be glamorous, but it can also be pernicious since it is the existing systems which keep the business going.

## C. THE CHARACTERISTICS OF MAINTENANCE

- One reason why maintenance costs are so high and are increasing is that changing programming code, once a system is operational, is very expensive, as shown in Exhibit II-5.

EXHIBIT II-2

GENERAL HARDWARE/SOFTWARE COST TRENDS



(Adapted from Barry Boehm)

EXHIBIT II-3

SOFTWARE DEVELOPMENT - MAINTENANCE TRADE-OFFS

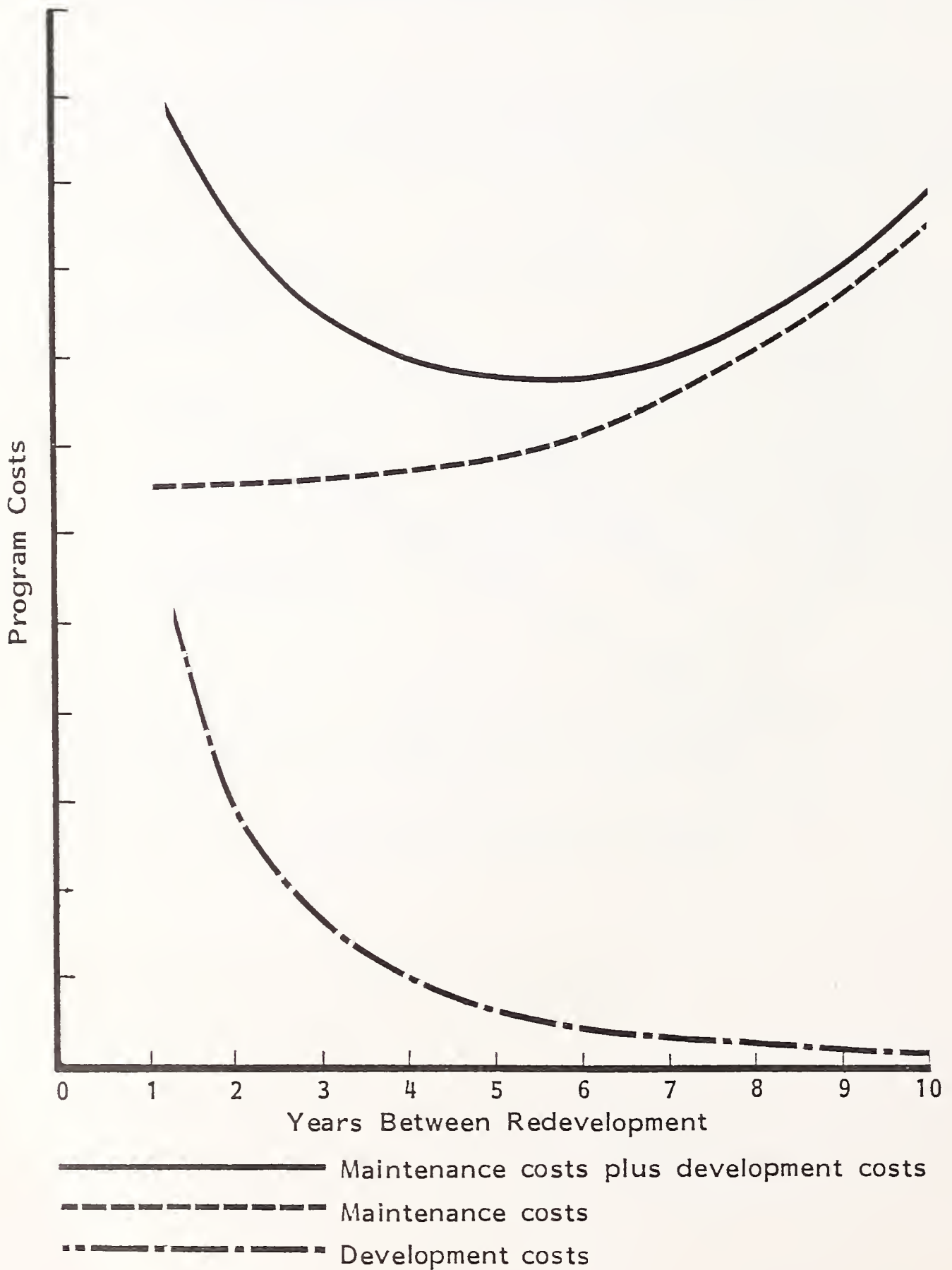
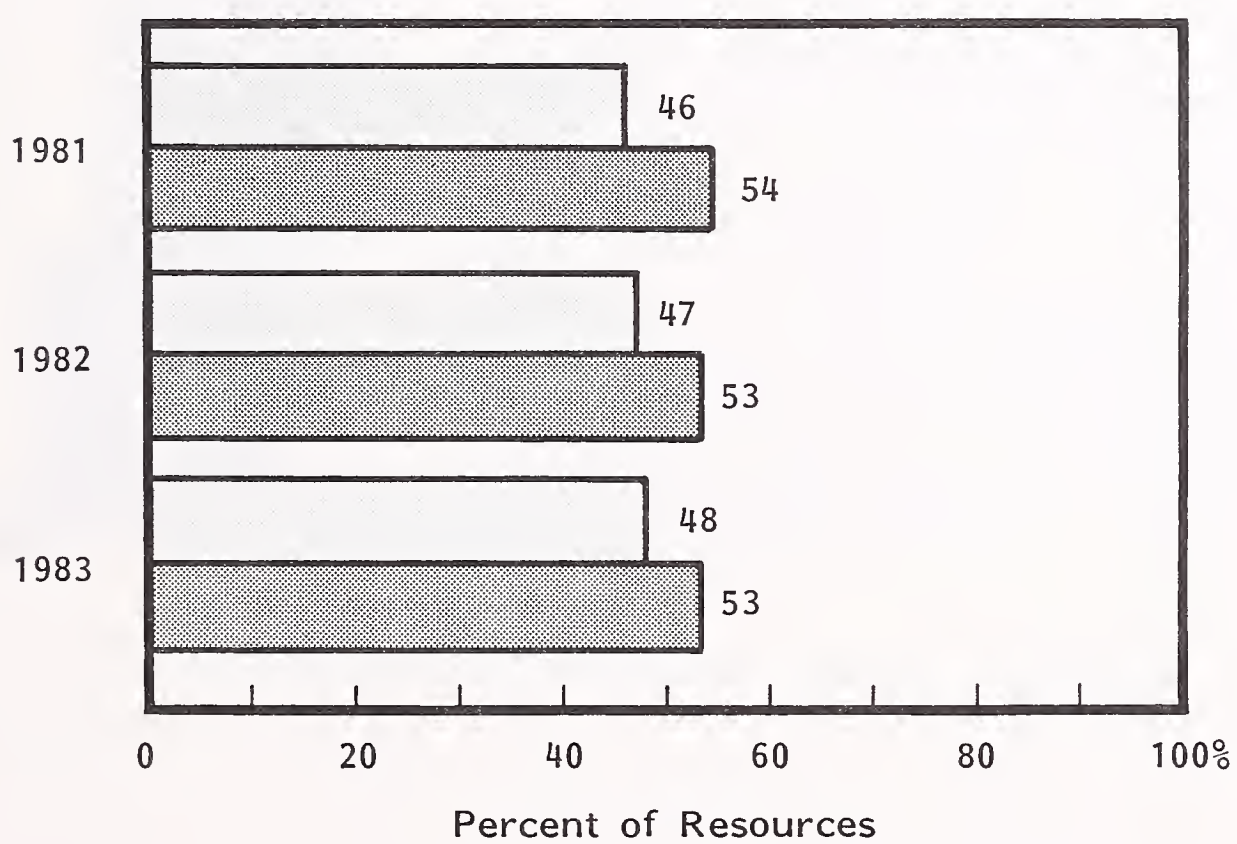


EXHIBIT II-4

NEW PROGRAM DEVELOPMENT VERSUS MAINTENANCE -  
1981-1983

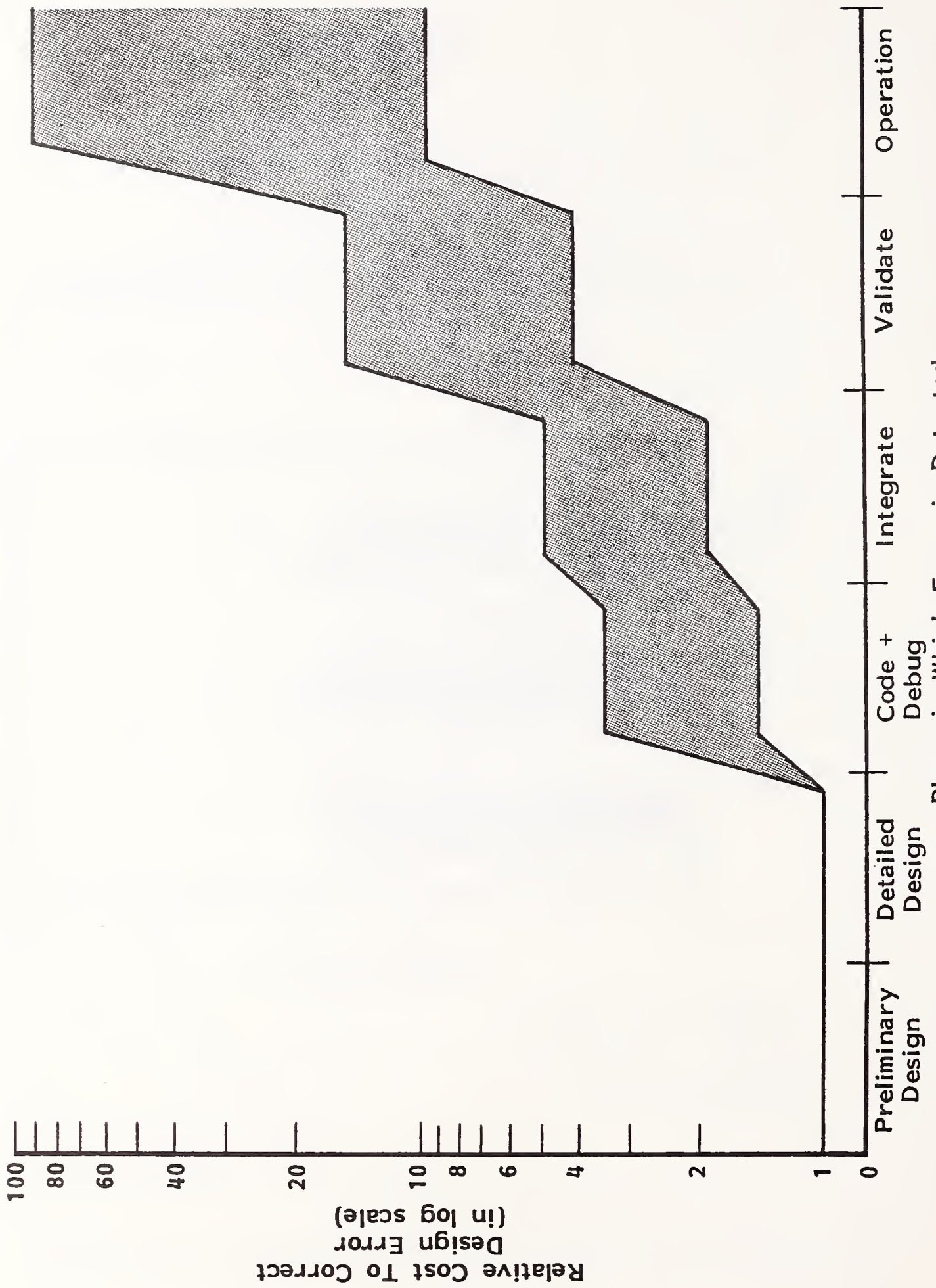


New Development  
 Maintenance

SOURCE: INPUT Survey

EXHIBIT II-5

SOFTWARE MODIFICATION COSTS IN DIFFERENT DEVELOPMENT STAGES



SOURCES: GTE, Bell Labs, IBM, TRW



- Maintenance is often identified solely with fixing software errors, but correction represents only 20% of software maintenance. Making functional enhancements accounts for about 65% of maintenance activities, as shown in Exhibit II-6. The other principal activity (15%) involves operational changes (conversions, housekeeping, efficiency improvement, etc.).
- There is a common misconception that software maintenance requires less effort and fewer skills than does software development. However, software maintenance may be more demanding than development, for example:
  - Documentation is necessary for thousands, perhaps millions, of lines of code to facilitate any future modifications or enhancements.
  - Unforeseen new requirements must be addressed.
  - There may be severe capacity and performance constraints.
  - The most visible software maintenance activities will be carried out during a crisis, e.g., fixing a critical bug.
- While the requirements are often more demanding in maintenance than in the development area, the resources to meet them are usually inferior.
- Software maintainers must work with obsolete languages that were often abandoned for good reasons.
  - Code that needs modification is often "tricky," e.g., the original programmer had to fit too many functions into a small space/time slot, and now the user wants to put in a few more, as shown in Exhibit II-7.
  - Much of the original programming is either poorly designed or inadequately coded.

EXHIBIT II-6

COMPONENTS OF SOFTWARE MAINTENANCE

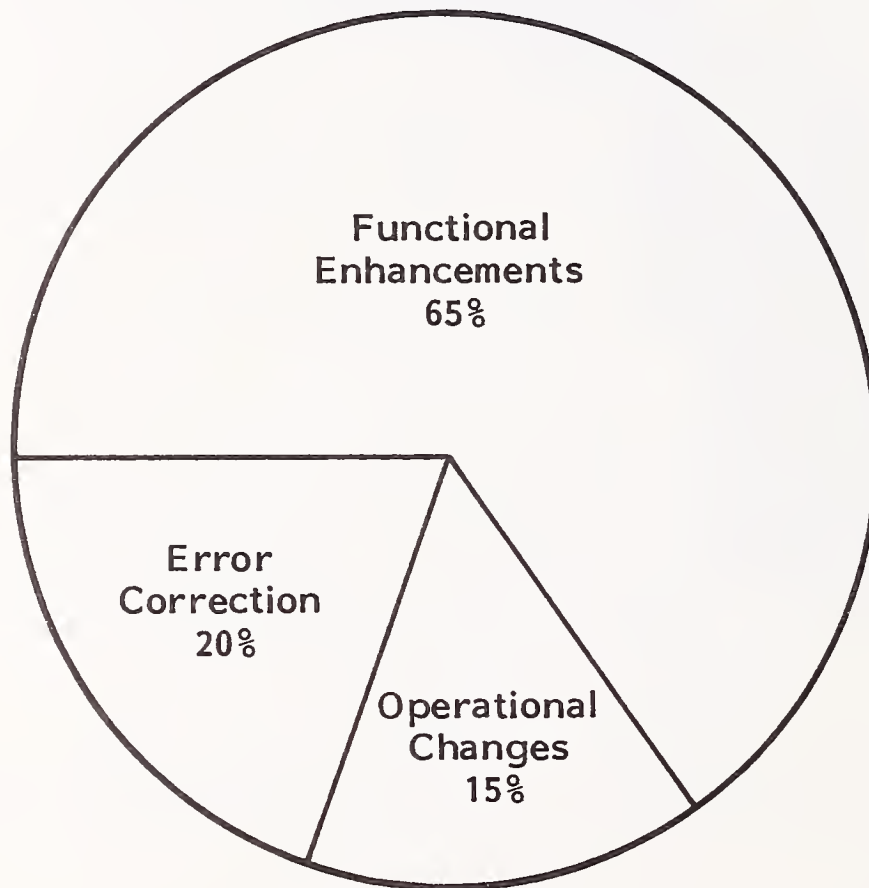
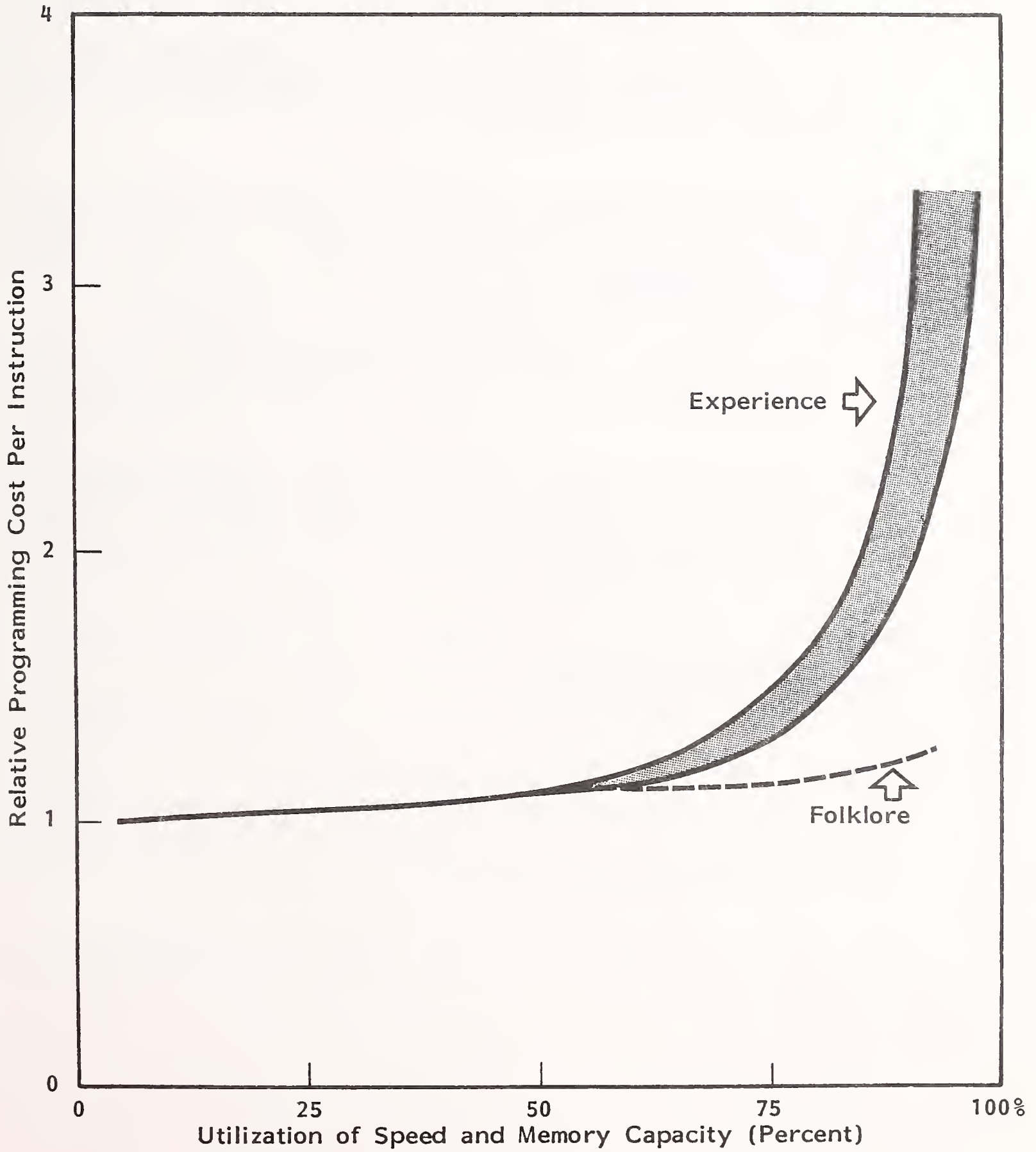


EXHIBIT II-7

CAPACITY LIMITATION EFFECTS ON MAINTENANCE COSTS



- Documentation is often poor, sometimes nonexistent.
- Productivity tools are even less advanced than those in the development area, and they are usually nonexistent.
- Maintenance is also unlike new development in that many maintenance problems did not have counterparts during the development phase, and therefore even the inadequate tools which are available to software developers will not apply, as shown in Exhibit 11-8.
- There are no methodologies or techniques available for the maintenance programmer. Has anyone, for example, ever heard of a maintenance analyst or a maintenance designer?
  - The maintainer is the last true programmer/analyst but is usually unrecognized as such!
  - It is indicative that the catalog of one of the leading data processing education firms which contains thousands of entries has no mention of software maintenance.

#### D. MAINTENANCE ELIMINATION

- Many managers say words to the effect that, "Yes, I have a maintenance problem now, but I expect it to decrease soon." On examination it turns out that they expect to reduce the problem by:
  - Having someone else solve it (i.e., the user or a vendor via software packages).

EXHIBIT II-8

COMPARISON OF MAINTENANCE AND NEW DEVELOPMENT

MAINTENANCE PROBLEM	A PROBLEM IN NEW DEVELOPMENT?	DEVELOPMENT TOOLS APPLICABLE?	SPECIFIC MAINTENANCE TOOLS AVAILABLE?
Obsolescent/ Obsolete Languages	No	No	No
Sophisticated "Tricky" Code	No	No	Minimal
Very Low Quality Code	Sometimes	No	No
Poor or Nonexistent Documentation	Rarely	No	Minimal
Externally Imposed Time Schedule	Sometimes	Partly	No

- Constructing such good future software that maintenance will be greatly reduced or at least made much easier (so easy, in fact, that users can do it).
- Packaged software is no panacea. Vendors and buyers of industry-specialized packages usually find that each company is just enough different that extensive software modifications are necessary. This causes the package to become unique and to need custom maintenance.
- Software can be made much easier to maintain by using the following:
  - Functional modules.
  - External parameters for constants.
  - Built-in, symbolic debugging codes.
  - A program design language (PDC) built into the program as comments.
- Debugging codes and PDC comments are the most useful for long-term maintenance, but they are the least used. Even when used, they are not cure-alls:
  - "Suspicious modules," which reject spurious inputs, can get out of synch.
  - There are so many variables, as in some insurance packages, for example, that volumes of documentation must be absorbed by users in order to specify those items which will never be used.
- The biggest threat to maintainable software is time/budget pressure to get something done or fixed as quickly as possible. No methodology can prevent that.

- Exhibit II-9 summarizes the reasons why maintenance will not be eliminated or even reduced much in the foreseeable future.
  
- There are four maintenance alternatives:
  - Do nothing.
  - Replace the system.
  - Overhaul the system.
  - Repair the function.
  
- Exhibit II-10 illustrates these relationships.
  - Doing nothing is an attractive alternative and is sometimes rational; however, it is usually not politically astute.
  - Replacing the system involves actions that are not usually considered maintenance.
  - The last two options, overhaul and repair, are the core of maintenance and will not go away.

EXHIBIT II-9

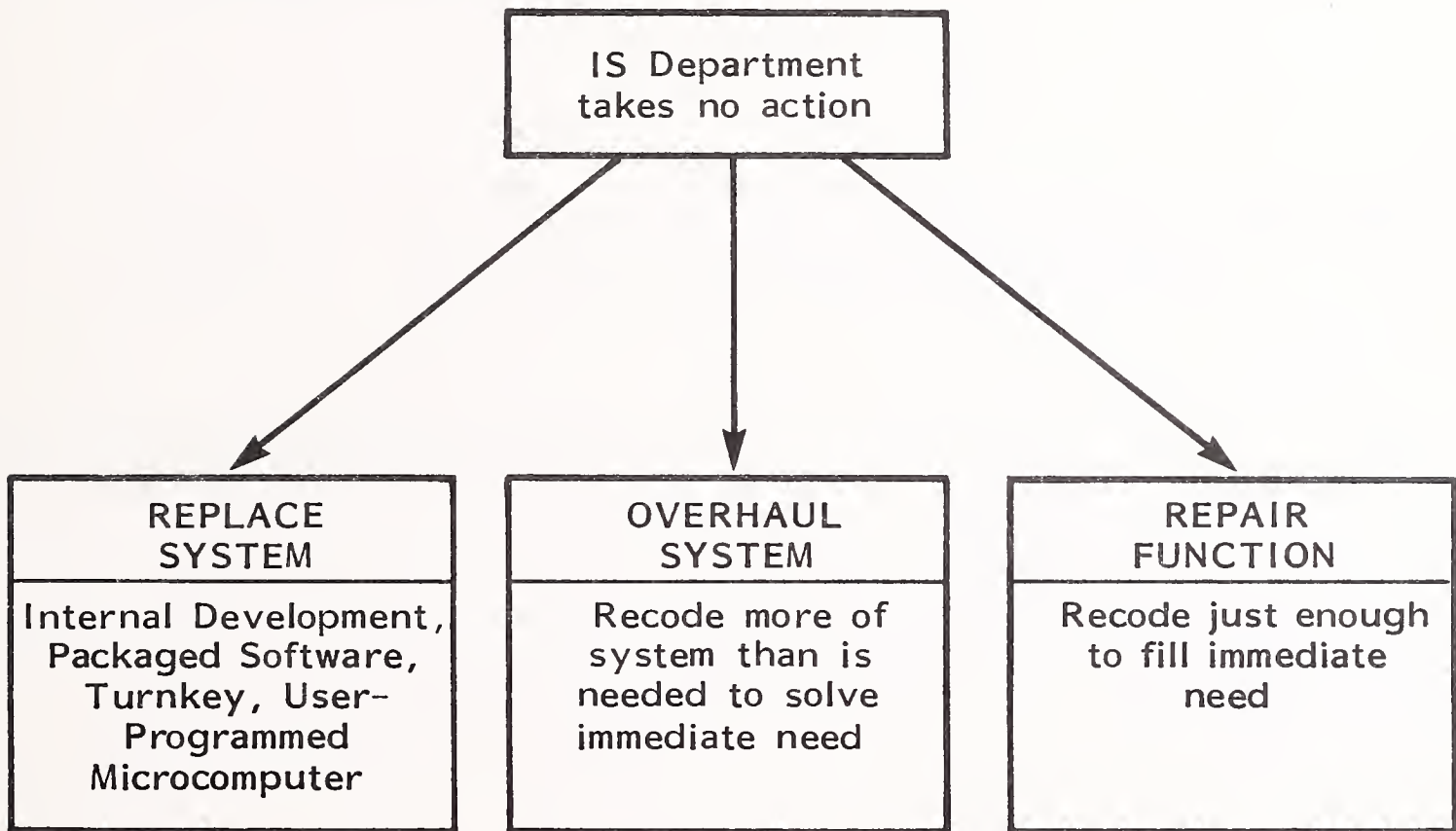
CAN MAINTENANCE BE ELIMINATED?

MAINTENANCE PREVENTIVE	ADVANTAGES	DRAWBACKS
Packaged Software	<ul style="list-style-type: none"> <li>● Vendor performs maintenance.</li> <li>● Often higher quality software.</li> </ul>	<ul style="list-style-type: none"> <li>● Buyer in applications strait-jacket (acceptable for general applications, often not acceptable for industry specific applications).</li> <li>● Buyer must maintain package interconnections.</li> </ul>
User Programming	<ul style="list-style-type: none"> <li>● User modifies software.</li> <li>● Especially good for report generation.</li> </ul>	<ul style="list-style-type: none"> <li>● Users cannot perform difficult jobs.</li> </ul>
Maintainable Software	<ul style="list-style-type: none"> <li>● Higher quality software needs less maintenance and is designed to ease maintenance.</li> </ul>	<ul style="list-style-type: none"> <li>● Time/budget pressures affect quality.</li> <li>● Standards often un-enforced.</li> <li>● Future needs must be understood.</li> <li>● Few maintainability definitions or principles exist.</li> </ul>



EXHIBIT II-10

MAINTENANCE ALTERNATIVES





### III MAINTENANCE INITIATIVES

- This chapter considers four areas where initiative may be taken to improve maintenance. It also analyzes trends and recommends actions.

#### A. TECHNICAL INITIATIVES

- There are, unfortunately, few technical solutions to maintenance (as cure, rather than prevention) on the horizon. There are three equally important reasons for this:
  - The bias against or inattention to maintenance makes tool developers look elsewhere.
  - There are at present few opportunities to apply to maintenance the relatively straightforward tools offered for programming development. Another problem is that development tools themselves are still often not used.
    - It is illustrative and illuminating that the Ada Programming Support Environment is almost totally directed to the development phase. This is in spite of the fact that weapons system software undergoes at least as many changes as commercial software and usually has a much longer required life.

- Maintenance is still a unique, problem-solving exercise, often more art than software engineering.
  - . For similar reasons, tools for systems analysis are still in an early stage of development.
- One relatively simple technical change only beginning to be used for maintenance is interactive debugging.
  - The relative lack of use (compared to development work) is largely due to prejudice and, to a certain extent, to a misunderstanding of maintainers' requirements.
  - The stated reason is that interactive debugging is too expensive, i.e., consumes too many machine cycles. This statement reveals a lack of appreciation for the true factors involved, i.e., personnel and opportunity costs.

## B. ADMINISTRATIVE CONTROL INITIATIVES

- Most companies perform various control and monitoring functions for the maintenance process, such as:
  - Problem and disposition reporting.
  - Priority requests and actions.
  - Maintenance scheduling and activity reporting.
  - Program change recording and control.
  - Documentation change control.

- Some of these, especially the program change recording and control, are at least semiautomated.
  - On an ad hoc basis some companies are trying to integrate these activities, which are steps in a common process.
- No commercial software product is yet available that will do this, although similar software is planned to control weapons systems software changes.
  - This is an area in which relatively simple software can do much to explicate the mysteries of maintenance, if management sets the priorities to make it happen.

### C. ORGANIZATIONAL INITIATIVES

- The organizational issues involved are:
    - How should maintenance be organized to do the work?
    - How should maintenance communicate with users?
- I. THE LOCATION OF THE MAINTENANCE FUNCTION
- There are three different approaches to creating an organization to perform maintenance:
    - Unitary: development and maintenance share roles within an application.
    - Independent: maintenance is set up as a separate function.

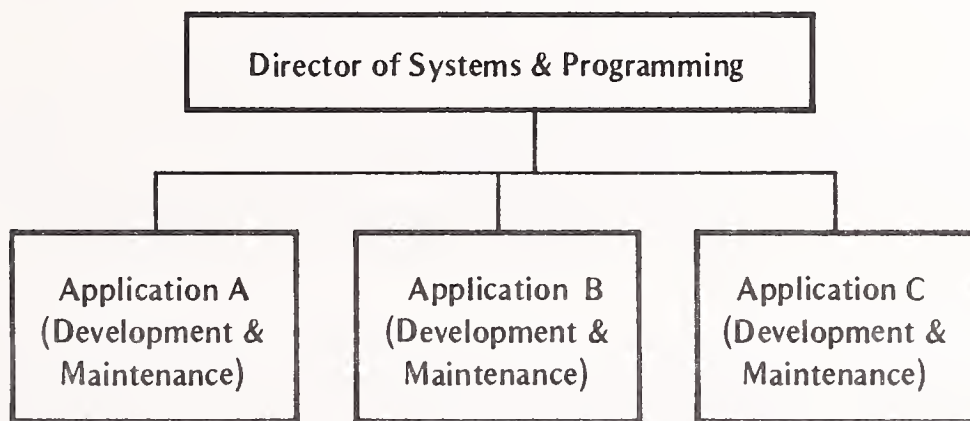
- Bifurcated: each application has a development and a maintenance function.
- Sample organization charts for each approach are shown in Exhibit III-1.
- The unitary approach is often used in small organizations and the bifurcated approach in large ones.
- The independent approach is little used, probably because of the bias against maintenance or, at the least, the lack of attention paid to maintenance.
  - This is in spite of the fact that the independent approach has the advantage of creating a career path for maintainers and has no serious disadvantages, as shown in Exhibit III-2.

## 2. USER COMMUNICATIONS

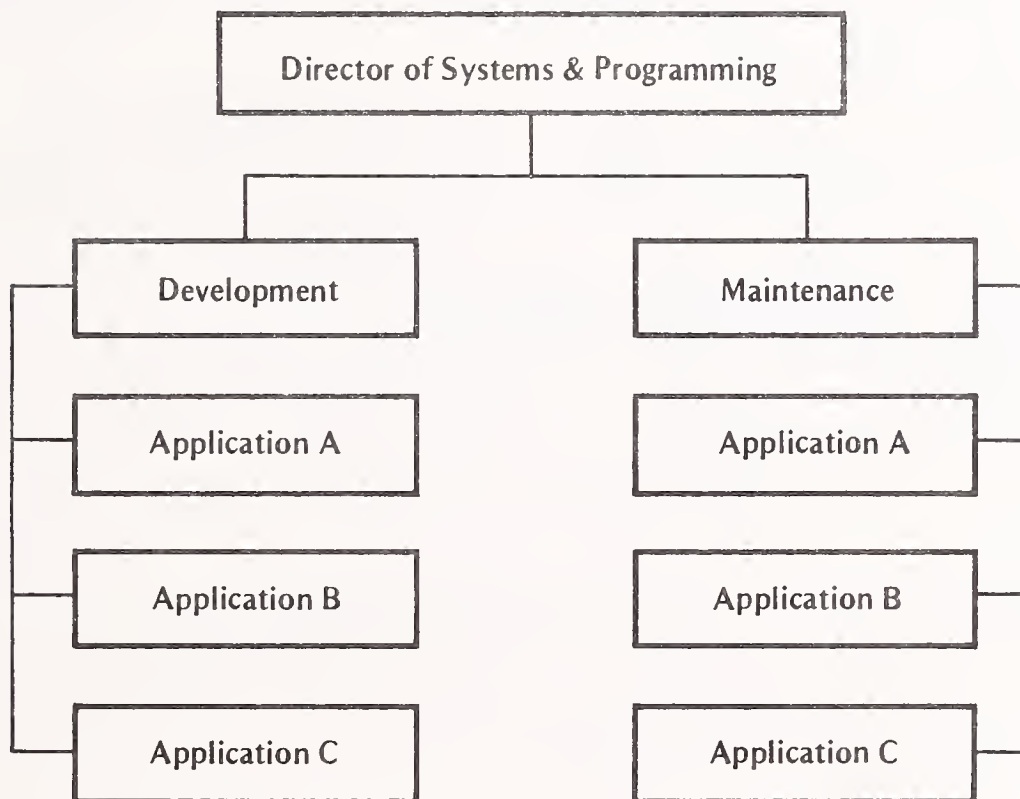
- IS management places much of the responsibility for maintenance problems on users' lack of knowledge or poor communications.
  - It is true that timely awareness of user needs is one of the key elements in developing an effective maintenance activity.
  - But there is a tendency in some IS organizations to blame users for problems and then take no effective steps to improve the situation (see INPUT's June 1982 report, Evaluating the EDP Level of Service).
- A few leading companies are setting up software support service centers to deal with customer questions. These are modeled after the centers (sometimes called "hot line" support) successfully operated by software vendors.
- A software support service center provides the following functions:
  - Screens and identifies software problems.

ALTERNATE MAINTENANCE ORGANIZATIONS

A: UNITARY



B: INDEPENDENT



C: BIFURCATED

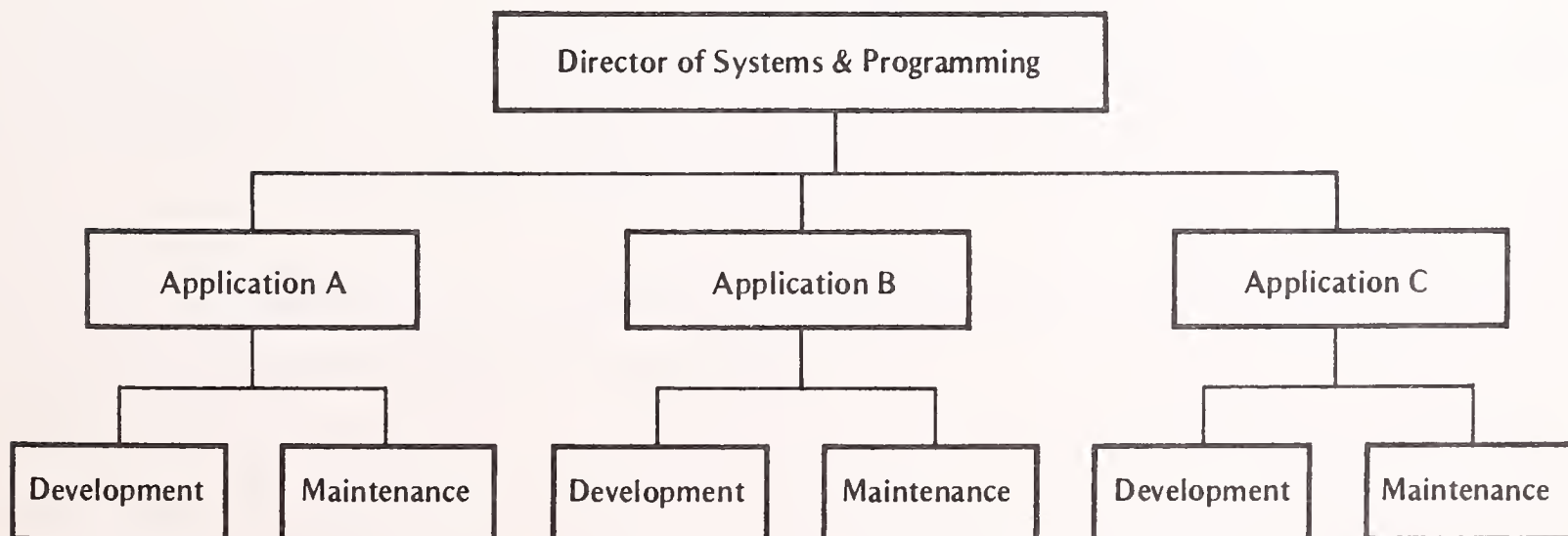


EXHIBIT III-2

ADVANTAGES AND DISADVANTAGES OF ALTERNATE  
MAINTENANCE ORGANIZATIONS

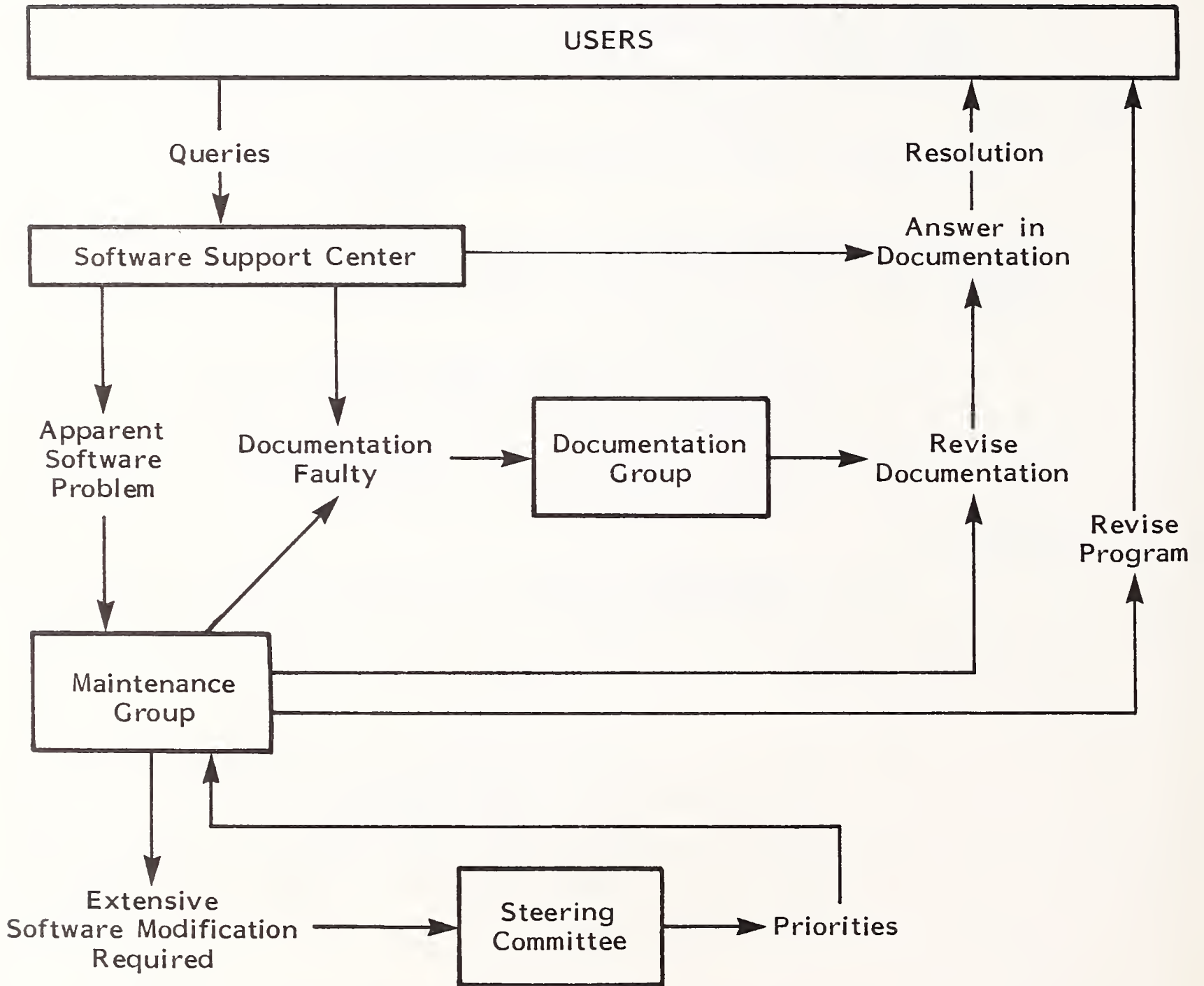
	UNITARY	INDEPENDENT	BIFURCATED
Advantages	<ul style="list-style-type: none"> <li>● Application flexibility</li> <li>● Application knowledge maximized</li> <li>● Defuses some of bias toward maintenance</li> </ul>	<ul style="list-style-type: none"> <li>● Career path for maintainers</li> <li>● Maintenance flexibility</li> </ul>	<ul style="list-style-type: none"> <li>● Application knowledge retained</li> </ul>
Disadvantages	<ul style="list-style-type: none"> <li>● Disgruntled specialists forced to do maintenance</li> <li>● Personnel scheduling more difficult</li> <li>● Maintenance specialists do not emerge</li> <li>● Large application groups difficult to manage</li> </ul>	<ul style="list-style-type: none"> <li>● Application knowledge split</li> </ul>	<ul style="list-style-type: none"> <li>● No career path for maintainers</li> <li>● Weakest performers end up in maintenance</li> </ul>



- Solves problems immediately by referring to the proper documentation source.
- Identifies defects in user documentation.
- Refers apparent software errors to maintenance staff.
- These functions and their relation to the maintenance group are shown in Exhibit III-3.
- There are pros and cons to using a software support center.
  - On one hand, a software support center will shield the maintenance group from many distractions that will waste time.
    - Many good programmers, especially good maintenance programmers, may not have the personal qualities required for, or the desire to cultivate, the public relations skills needed in a customer support role.
  - On the other hand ongoing user contact with the maintenance staff is desirable to keep informed, formally and informally, on user needs and interests.
    - While an initial question might not be very important, follow-up conversation may uncover questions or needs that would not surface formally for many months. Awareness of these developing needs may influence the manner in which other maintenance tasks are approached.
- In many cases the choice of the correct alternative will flow naturally out of a particular system's characteristics.

EXHIBIT III-3

A SOFTWARE SUPPORT CENTER



- Small systems and small organizations have neither the need nor the budget for a formal software support center. A single person should, however, be designated as the principal contact.
- Large systems, especially those in large organizations, will often find formal structure useful and comfortable in their organizational context.
- IS departments, especially in large organizations, should remember that the customer support centers of major vendors are large and complex. Exhibit III-4 shows the typical organizational communication flow of such a vendor.
  - The "front line" customer support personnel are trained to handle a broad range of software questions, often across several software products. Over half of all vendor customer maintenance problems are caused by ignorance of the product's capabilities or misuse of the product, as shown in Exhibit III-5. Consequently, vendor customer support staff need only know the documentation well to handle many queries.
  - The second line of defense is specialized software support technicians who back up the customer contact staff. The technicians may specialize by product, subproduct, or function (e.g., communications, data base management, graphics interfaces). The customer support staff knows which technicians specialize in which areas and refers questions appropriately.
  - When a software error or potential modification is involved, the product maintenance staff comes into play to identify the precise problems and, if required, to make programming changes. On some occasions the development staff may become involved also.

EXHIBIT III-4

MAINTENANCE COMMUNICATIONS IN A  
SOFTWARE VENDOR ENVIRONMENT

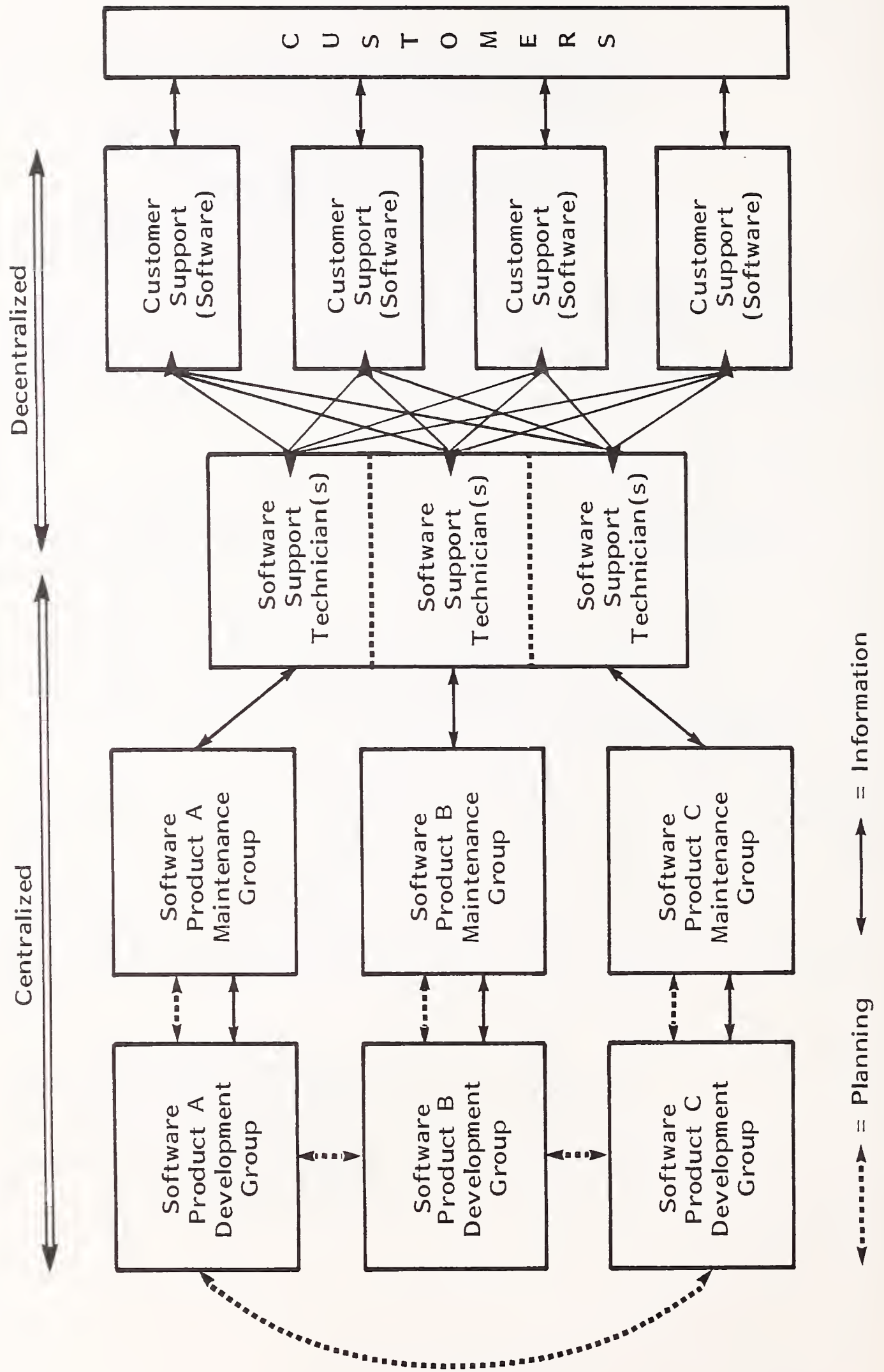
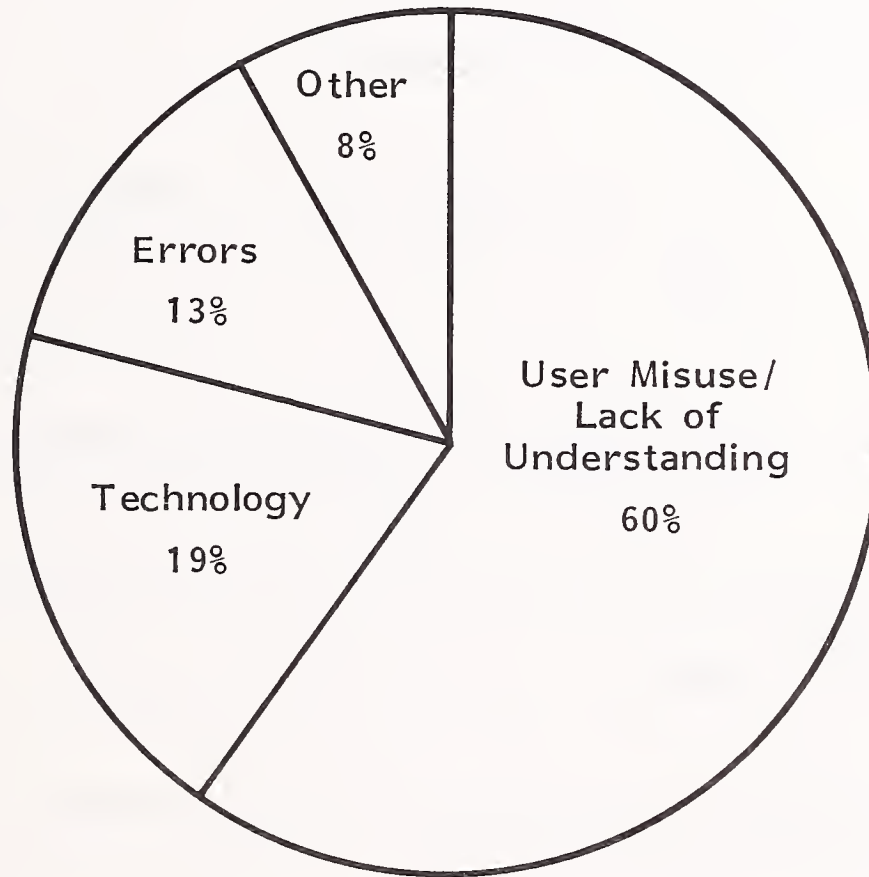


EXHIBIT III-5

FREQUENCY OF MAINTENANCE ACTIVITIES



SOURCE: INPUT Survey

## D. PERSONNEL AND MANAGEMENT INITIATIVES

- The three preceding maintenance areas, technical, administrative and organizational, are all important and all have room for significant progress. But nothing will be accomplished without proper management and personnel policies.
  - Quite simply, little is happening in maintenance today because many managers wish it would go away.
    - How else can we explain the assignment of the least qualified (trainees and incompetants) to the most demanding of software tasks?
    - IS management intellectually comprehends the primacy of maintenance tasks but usually does not act on that knowledge.
- IS management must treat maintenance and its practitioners seriously. Positive actions include:
  - Managing maintenance as a separate operation, organizationally and intellectually.
  - Teaching maintenance techniques within the organization.
  - Maintenance careers for the right people should be encouraged rather than implicitly discouraged, as the case is now.
    - A career path and status rewards are most important.
    - The lack of order associated with maintenance really represents an intellectual challenge. If this is recognized by management, it will soon be accepted by much of the organization.

- Special monetary rewards should not be established; this will only further the "hazardous duty" image. Rather, maintenance staff should be eligible for all the rewards and recognition available to any other programmer or analyst.

## E. CONCLUSION

- There are many forces pushing to increase required maintenance resources:
  - Old systems are harder to maintain.
  - New systems lengthen the maintenance "tail."
  - Interlinked software adds to maintenance complexity.
  - Distributed systems add to maintenance difficulty.
  - User systems add more maintenance players.
- The initial steps required to improve maintenance in an organization are management initiatives:
  - Separate maintenance from development.
  - Establish a support center.
  - Improve information about and control of the maintenance function. This will often require a modest investment in tailored software.

- Encourage the development and retention of skilled maintenance specialists. Initially, train through apprenticeship to spread good maintenance practices throughout the organization.
- Technical advances in maintenance will begin to flow automatically from having maintenance specialists.
- The Department of Defense sponsored R&D should be of some longer-term assistance, i.e., the Ada support environment and work being supported by the Rome (NY) Air Development Center.
- The outlook for commercially developed maintenance tools is not as bright.







**MANAGEMENT PROGRAMS:** Designed for clients with a continuing need for information about a range of subjects in a given area.

- Management Planning Program in Information Systems - Provides managers of large computer/communications facilities with timely and accurate information on developments which affect today's decisions and plans for the future.
- Management Planning Program for the Information Services Industry - Provides market forecasts and business information to software and processing services companies to support planning and product decisions.
- Company Analysis and Monitoring Program for the Information Services Industry - Provides immediate access to detailed information on over 3,000 companies offering turnkey systems, software and processing services in the U.S. and Canada.
- Management Planning Program in Field Service - Provides senior field service managers in the U.S. and in Europe with basic information and data to support their planning and operational decisions.
- On-Target Marketing - A practical, "how-to-do-it" methodology for more effective marketing problem solving and planning delivered to clients via workshops and/or consulting services.

**MULTICLIENT STUDIES:** Research shared by a group of sponsors on topics for which there is a need for in-depth "one-time" information and analysis. A multiclient study typically has a budget of over \$200,000, yet the cost to an individual client is usually less than \$30,000. Recent studies specified by clients include:

- Selling Personal Computers to Large Corporations
- Improving the Productivity of Systems and Software Implementation
- User Communication Networks and Needs
- Improving the Productivity of Engineering and Manufacturing Using CAD/CAM

**CUSTOM STUDIES:** Custom studies are sponsored by a single client on a proprietary basis and are used to answer specific questions or to address unique problems. Fees are a function of the extent of the research work. Examples of recent assignments include:

- Organizing for Effective Software Development
- Investigation of TSO and Comparable Systems
- Corporate Plan for Utilizing CAD/CAM
- 1981 ADAPSO Survey of the Computer Services Industry
- Analysis of Business Services for a Major Financial Institution
- Study of the Specialty Terminal Market
- Evaluate Information Industry Innovations

# ABOUT INPUT

INPUT provides planning information, analysis, and recommendations to managers and executives in the information processing industries. Through market research, technology forecasting, and competitive analysis, INPUT supports client management in making informed decisions. Continuing services are provided to users and vendors of computers, communications, and office products and services.

The company carries out continuous and in-depth research. Working closely with clients on important issues, INPUT's staff members analyze and interpret the research data, then develop recommendations and innovative ideas to meet clients'

needs. Clients receive reports, presentations, access to data on which analyses are based, and continuous consulting.

Many of INPUT's professional staff members have nearly 20 years' experience in their areas of specialization. Most have held senior management positions in operations, marketing, or planning. This expertise enables INPUT to supply practical solutions to complex business problems.

Formed in 1974, INPUT has become a leading international consulting firm. Clients include over 100 of the world's largest and most technically advanced companies.

---

## OFFICES

### Headquarters

P.O. Box 50630  
Palo Alto, California 94303  
(415) 493-1600  
Telex 171407

### Dallas

Campbell Center II  
8150 N. Central Expressway  
Dallas, Texas 75206  
(214) 691-8565

### New York

Park 80 Plaza West-1  
Saddle Brook, New Jersey 07662  
(201) 368-9471

### United Kingdom

INPUT, Ltd.  
Airwork House (4th Floor)  
35 Piccadilly  
London, W. 1.  
England  
01-439-4442  
Telex 269776

## AFFILIATES

### Australia

Infocom Australia  
Highland Centre, 7-9 Merriwa St.,  
P.O. Box 110,  
Gordon N.S.W. 2072  
(02) 498-8199  
Telex AA 24434

### Italy

PGP Sistema SRL  
20127 Milano  
Via Soperga 36  
Italy  
Milan 284-2850

### Japan

Overseas Data Service Company, Ltd.  
Shugetsu Building  
No 12 - 7 Kita Aoyama  
3-Chome Minato-ku  
Tokyo, 107  
Japan  
(03) 400-7090  
Telex J26487

### Sweden

P.O. Persson Konsult AB  
Box 221 14  
Hantverkargatan 7  
104 22 Stockholm  
Sweden  
08-52 07 20



