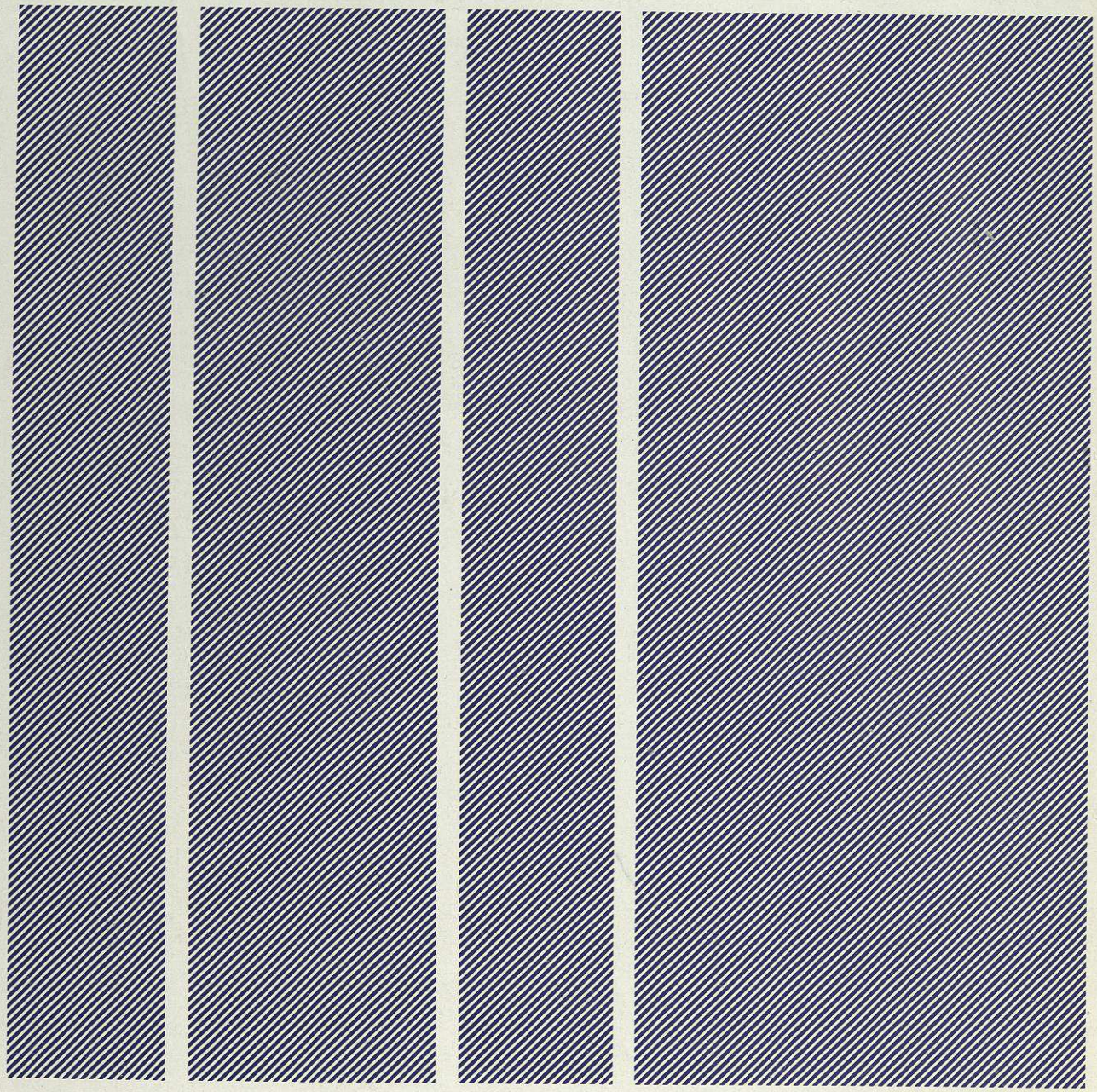
Report Series
No. 33

Managing Operational Computer Services

January 1983



The Butler Cox Foundation

THE BUTLER COX FOUNDATION

REPORT SERIES NO. 33

MANAGING OPERATIONAL COMPUTER SERVICES

ISSUED JANUARY 1983

Abstract

In this report the term 'computer services' refers to that part of the information systems function that is responsible for the day-to-day operation of all (or most) of an organisation's computer-based resources (including telecommunications resources). The report shows that operations is becoming a much more important and visible component of the information systems function.

The purpose of the report is to emphasise the ways in which the responsibilities of the computer services function are changing, and to highlight the key issues for the effective management of computer services in the 1980s.

Research team

The team that researched and wrote this report was:

Jim O'Connor, a senior consultant with Butler Cox specialising in all aspects of information systems management. His background includes positions in systems and data processing management both in the United Kingdom and the United States.

Rob Moreton, a consultant with Butler Cox specialising in system development and data processing management. He has lectured extensively on these topics and has contributed to the research programmes of several Foundation reports.

Acknowledgement

The staff of the Foundation wish to thank the many computer services managers from a wide diversity of organisation who assisted in the research for this report.

In drafting chapter 4 of this report we have drawn extensively on material from a research study carried out by Butler Cox & Partners on behalf of the Amdahl Corporation. We are grateful for Amdahl's permission to use this material, which was published originally in April 1982 in a report entitled "Computer Disasters and Contingency Planning". Copies of that report may be obtained direct from Amdahl (UK) Ltd.

Photoset and printed in England by Flexiprint Ltd., Worthing, Sussex.

THE BUTLER COX FOUNDATION

Butler Cox & Partners
Butler Cox is an independent management consultancy and research organisation, specialising in the application of information technology within commerce, government and industry. The company offers a wide range of services both to suppliers and users of this technology. The Butler Cox Foundation is a service operated by Butler Cox on behalf of subscribing members.

Objectives of The Foundation
The Butler Cox Foundation sets out to study on behalf of subscribing members the opportunities and possible threats arising from developments in the field of information systems.

The Foundation not only provides access to an extensive and coherent programme of continuous research, it also provides an opportunity for widespread exchange of experience and views between its members.

Membership of The Foundation
The majority of organisations participating in the Butler Cox Foundation are large organisations seeking to exploit to the full the most recent developments in information systems technology. An important minority of the membership is formed by suppliers of the technology. The membership is international with participants from Belgium, Denmark, France, Italy, the Netherlands, Sweden, Switzerland, the United Kingdom and elsewhere.

The Foundation research programme
The research programme is planned jointly by Butler Cox and by the member organisations. Half of the research topics are selected by Butler Cox and half by preferences expressed by the membership. Each year a short list of topics is circulated for consideration by the members. Member organisations rank the topics according to their own requirements and as a result of this process, members' preferences are determined.

Before each research project starts there is a further opportunity for members to influence the direction of the research. A detailed description of the project defining its scope and the issues to be addressed is sent to all members for comment.

The report series
The Foundation publishes six reports each year. The reports are intended to be read primarily by senior and middle managers who are concerned with the planning of information systems. They are, however, written in a style that makes them suitable to be read both by line managers and functional managers. The reports concentrate on defining key management issues and on offering advice and guidance on how and when to address those issues.

Additional report copies
Normally members receive three copies of each report as it is published. Additional copies of this or any previous report (except those that have been superseded) may be purchased from Butler Cox.

Previous reports
No. 1 Developments in Data Networks
No. 2 Display Word Processors*
No. 3 Terminal Compatibility*
No. 4 Trends in Office Automation Technologies
No. 5 The Convergence of Technologies
No. 6 Viewdata*
No. 7 Public Data Services
No. 8 Project Management
No. 9 The Selection of a Computerised PABX
No. 10 Public On-line Information Retrieval Services*
No. 11 Improving Systems' Productivity
No. 12 Trends in Database Management Systems
No. 13 The Trends in Data Processing Costs
No. 14 The Changing Equipment Market
No. 15 Management Services and the Microprocessor
No. 16 The Role of the Mainframe Computer in the 1980s
No. 17 Electronic Mail
No. 18 Distributed Processing: Management Issues
No. 19 Office Systems Strategy
No. 20 The Interface Between People and Equipment
No. 21 Corporate Communications Networks
No. 22 Applications Packages
No. 23 Communicating Terminals
No. 24 Investment in Systems
No. 25 System Development Methods
No. 26 Trends in Voice Communication Systems
No. 27 Developments in Videotex
No. 28 User Experience with Data Networks
No. 29 Implementing Office Systems
No. 30 End-User Computing
No. 31 A Director's Guide to Information Technology
No. 32 Data Management
**These reports have been superseded.*

Future reports
No. 34 Strategic Systems Planning
No. 35 Multifunction Equipment
No. 36 Cost-Effective Systems Development and Maintenance

THE BUTLER COX FOUNDATION

REPORT SERIES NO. 33

MANAGING OPERATIONAL COMPUTER SERVICES

CONTENTS

MANAGING OPERATIONAL COMPUTER SERVICES

REPORT SYNOPSIS

The scope of the 'operations' part of commercial data processing is broadening and changing, primarily because of technological developments in the structure and delivery of systems. For computer services managers this development poses both threats and opportunities. In particular, managers must deal with the basic changes that are occurring in the roles of their computer services staff. And the managers themselves need to gain new skills in order to relate effectively to the business needs of the organisation.

In broad terms, we address two key questions in the report. First, what are the changes? Second, what should the computer services manager do about them? From the comprehensive review provided, managers can select those factors which apply to their own organisations.

Five significant areas of technological change are identified in chapter 1: database management systems, online and distributed system architectures, data communications, more reliable hardware and more resilient system architectures. These have a direct impact in their own right on the computer services department, but also an indirect impact via their effect on the attitudes of users of the department's services.

Because of these technological changes, users increasingly depend on the performance of their information systems. As a result, the perceived importance of the computer services department has been raised, and computer services has become a critical component of the commercial organisation.

Within the computer services department itself there are changing responsibilities. In addition to the traditional 'operations' role, new roles in user support and development support have emerged which require higher-calibre computer services staff to be recruited. Skilled staff are now increasingly used to inject operations expertise into development projects, and to provide development-related services such as production support programming and application package support.

The implications of these changes for computer services personnel are discussed in chapter 2, which shows that traditional jobs are disappearing and new roles are being created. Nevertheless, simple retraining from one category to the other is not possible because different skills and personal attributes are required. In the past the typical computer services department consisted mainly of relatively unskilled people. Now the pattern is changing: fewer staff will be required, but they will be more skilled. Achieving this transformation successfully is probably the most difficult challenge facing computer services management. In particular, fewer computer operators will be required as their traditional tasks are increasingly automated. This will pose a difficult problem for managers in the future, though they have a breathing space at present before automated operations are introduced widely.

Most computer operators will not be well suited to the new positions that are being created, such as those of operations analyst, technical support specialist and end-user support specialist. Compared with traditional operators, applicants for these jobs will need more technical knowledge, higher educational standards, greater intellectual ability, more initiative, and the ability and desire to relate more closely to the general business aims of the organisation.

But these new specialists will also have to step in as required to sort out infrequent, but critical operational problems. Organising the department with this in mind is a major management problem. Another important factor is that the boundaries between computer services and system development responsibilities will become increasingly blurred.

These in essence are the sort of changes that are occurring; how should managers respond? In chapter 5 the answer to this question is condensed into five broad guidelines:

—Prepare for a changing computer services environment.

—Implement a continuing evaluation process.

—Implement a risk-control programme.

—Develop general management skills.

—Beware of complacency.

In preparing for the *changing environment,* the four main areas of change on which to concentrate are computer operations techniques, telecommunications, system architectures and new support roles. Early planning for automated operations will minimise disruption later; and in moving towards integrated telecommunications services a sound grasp of the emerging options will be needed in order to match facilities to the needs of the business. The computer services manager must keep abreast of concepts in distributed processing and online systems so as to help shape their application in his organisation; and he must ensure that his department is prepared and equipped to suport end users and systems development staff.

Continuing evaluation is crucial in ensuring that the services provided continue to meet the needs of the organisation. Hardware performance monitoring is no longer sufficient; the need (as pointed out in chapter 3) is for a comprehensive assessment of the overall effectiveness of the service. This can lead to remarkable savings and other benefits, provided a formal procedure is followed and the analysis is truly objective. Few organisations, it appears, are taking advantage of these techniques at present.

Risk control is another key area where assessment of the vulnerability of the computer services is vital to the well-being of the organisation. The threats of possible interruptions to the services and of unauthorised use have become more serious as the importance and complexity of the services have grown, and as users have become more dependent on them. Chapter 4 describes the risks, the potential losses, and the principles of implementing a formal risk-control programme, including contingency planning. In the absence of such a programme, computer services managers cannot say with confidence that the level of service integrity they provide is adequate. Absolute security is impossible, but an acceptable level of protection can — and should — be provided. Proper contingency planning in particular has been neglected by many organisations, which tend to relegate such planning to a secondary position behind the day-to-day business of getting the primary job done. This is understandable, but dangerous.

Computer services managers should develop *general management skills* because (as chapter 2 shows) their own role is changing just as significantly as those of their staff. The computer services manager is no longer simply a 'chief engineer' who keeps the machinery running. Now he is increasingly regarded as a key person in the information system decision-making process, with wider responsibilities and a significant contribution to make. This implies a new emphasis on general management skills as distinct from technical skills. He still needs a good understanding of the 'operations' or 'production' duties — and, indeed, of the new techniques of technical support, database administration, user support and development support. But above all he must be able to deal confidently with the organisation's mainline business managers. He needs to be aware of impending developments, both in systems and in terms of the overall business, and to organise his department so as to contribute positively to systems planning and development.

Finally, because computer services managers operate in an ever-changing environment they must *avoid complacency.* Users' needs, and their perceptions of an acceptable service, will continue to change. A service that is adequate today will be unacceptable tomorrow. By anticipating change, computer services managers can ensure that its effects are positive and beneficial — but this will demand honesty and planning.

PREFACE

From the early days of commercial data processing until the beginning of this decade the typical data processing department was usually organised into two major and distinct sections — a systems and programming department and an operations department. For many years the responsibilities of, and the relationship between, these two sections varied very little. The operations department was responsible for providing the computing power that the systems and programming department needed to satisfy the demands of corporate users. In many respects, the operations department was subservient to the systems and programming department and, as a consequence, its role was not very visible to the organisation at large.

This situation is now changing. The role of data processing operations is becoming a much more important and visible component in the total information systems equation. In many organisations the operations role has broadened to such an extent that it is now just one part of a newly evolved support-oriented organisation. This new organisation is typically referred to by titles such as computer services, production services, or even as 'data processing'.

For the purpose of this report we use the term 'computer services' to refer to that part of the information systems function that is responsible for supporting on a day-to-day production basis all (or most) of an organisation's computer-based resources. It does not include the systems development aspects of information systems.

The purpose of this report

The purpose of this report is to focus the attention of corporate and information systems management on the ways in which the computer services function is currently changing, and will continue to change throughout the 1980s. The report highlights the key issues for the effective management of the computer services function in the 1980s.

The scope of the report

The report reviews those aspects of computer services management that are changing most rapidly in medium to large-scale organisations in Western Europe. We have placed particular emphasis on the following issues:

- —The changing relationships between computer services and other corporate functions.
- —The changing responsibilities of computer services within the information systems environment.
- —The effects those changes have on the personnel requirements for computer services.

The report does not consider in detail the various operations and management techniques and tools that are available. Instead, it concentrates on the evolving nature of the computer services function, and examines the alternative approaches and solutions to the problems that are created by this evolving environment.

The structure of the report

Chapter 1 first discusses the changing nature of the computer services function from a technological point of view and from the users' point of view. It then reviews the changing responsibilities of the computer services department — changes brought about largely by the growing importance of computer services. Chapter 2 then highlights the personnel issues arising from the changing nature of computer services. In particular it shows that there will be a diminishing requirement for traditional computer operators and a growing requirement for more specialised roles.

In chapter 3, we identify the key factors that need to be taken into account when measuring the effectiveness of the computer services department, and propose a methodology for carrying out such an evaluation.

Chapter 4 discusses the potential threats to the integrity of computer services and identifies the potential losses that can result from a breakdown in the services. It also provides guidelines for carrying out a risk-control programme and for preparing contingency plans. Finally, in chapter 5, we present a concise set of guidelines for the effective management of the computer services function.

CHAPTER 1

THE CHANGING NATURE OF COMPUTER SERVICES

The commercial information systems function has had to contend with many far-reaching changes in recent years. Radical changes in processing architectures and in system development methodologies are but two examples. Changes such as these have had a significant impact on the nature of the work performed within the information systems function as a whole and, in particular, within the computer services component of information systems.

In this chapter we explore the evolving nature of the computer services function. We begin by examining the two pressures that are the driving force behind the evolutionary process — technological changes and changes in users' attitudes towards the importance of information systems. We then discuss the ways in which the responsibilities of the computer services function are changing in response to these pressures.

TECHNOLOGICAL CHANGES

Our research identified the five most significant areas of technological change that have impacted (and will continue to impact) on the nature of the work performed by computer services as:

— Database management systems.

— Online and distributed system architectures.

— Data communications.

— More reliable hardware.

— More resilient system architectures.

Database management systems

Foundation Report No. 32 (Data Management) established that most large organisations now make use of a database management system, and this finding was borne out by the user organisations that we spoke to during the research for this report. The use of database management systems had affected the computer services function in two main ways:

— Operations staff now have less direct involvement in the physical allocation and maintenance of disc space because many of these tasks are handled automatically by the database management system. As a result, the workload of operations staff has reduced, sometimes significantly.

— In a database environment, there is an increased need for a technically oriented database administration function. Some organisations have allocated this responsibility to the computer services department. (The role of the database administrator is discussed in Report No. 32.)

Online and distributed system architectures

The mix of application systems used by a typical commercial organisation is no longer based exclusively on centralised batch technology. Computer services departments now provide a service that has an increasingly large online and distributed system component, and in some organisations batch processing is now the exception. The trend toward online and distributed systems is likely to continue for the foreseeable future. The concensus of opinion from our research was that batch systems will always exist in some form, but more and more they will be used to perform the non time-critical number crunching and batch file update functions for which they are best suited.

Online systems

Replacing batch systems by online systems affects the computer services department in two main ways. First, computer operations staff have less direct day-to-day interaction with an online system because the systems' users initiate and control the input and extraction of information. Second, transferring responsibility for data input and control to the user has led to a greater need for interaction between users and the computer services department. Most of this interaction is required to answer queries and to solve immediate problems relating to the use of online systems.

The overall effect is for the computer services department to concentrate less on handling system inputs and outputs, or on controlling systems directly, and more on direct user support. As a consequence, fewer computer services personnel are required to process the data and those who are required need better interpersonal skills than before.

Distributed computing

The increasing use of distributed computing affects the computer services department in a similar way to the use of online systems. The two techniques often go hand-in-hand because, when part of a central mainframe's workload is distributed to a remote loca-

tion the transferred applications are quite often converted (at least partially) to online techniques. This conversion is usually necessary either to overcome the lack of local data entry and data despatch facilities or to do away with them.

Remote processors, as distinct from remote access to a central processor, generate an additional set of problems for the computer services department. Despite suppliers' claims to the contrary, most minicomputers do not run themselves. Some form of localised operations support is usually needed to handle problems as diverse as communication line failures, restarts after a power failure, disc head crashes, and even such mundane tasks as security backups. Some of these problems can be resolved over the telephone, but many cannot. User personnel can be trained to handle these tasks, but that is no different from having a local computer operator.

Data communications

The growth in the use of online and distributed systems means that data communications now forms an increasingly important element of information systems. The responsibility for managing data communications was allocated traditionally to the computer operations department, and in smaller organisations it has remained there. Other organisations have established a separate data communications group as part of the computer services department, operating in parallel to, but separate from, the operations department. A small number of organisations have allocated the responsibility for data communications to an authority completely outside the data processing environment.

In our survey, those organisations that had located the data communications responsibility in the computer services department had done so for one or more of the following reasons:

—Because data communications is a hardware-based resource that has direct physical links with the data processing resource.

—Because developments in data communications hardware technology are increasingly based on and linked to developments in computer hardware.

—Because the data communications resource is a primary vehicle for delivering information processing power (via online systems and distributed processing architectures). As such, it makes sense for it to be controlled by the organisation that controls the other delivery vehicles, such as printed outputs.

In addition, the network management function in many organisations is linked closely with systems programming. The two roles often are located within the computer services department as a single technical support group, but with each discipline as a co-equal half of the group. This link had usually been established because each of the disciplines needed easy and constant access to knowledge about the other in order to function properly, but each was too complex to become subservient to the other.

Those organisations that had allocated the data communications responsibility outside the computer services department had usually done so either because they had a relatively complex network, or because of political or geographic circumstances.

More reliable hardware

The reliability of computer hardware has improved considerably during the past decade. This improvement has been caused by better hardware design and manufacturing processes and by competition from plug compatible manufacturers. In the past, computer services managers had to devote a substantial proportion of their time to making sure that the hardware was running when users needed it, and to recovering from the crises caused by machine breakdowns. The more reliable hardware now available enables them to devote more of their time to ensuring that they are providing an efficient and effective service.

Another contributory factor has been the improved standard of hardware maintenance services provided by the suppliers. Despite the large increase in the installed processor base, most computer services managers in our survey believed that the quality of maintenance services was adequate. Two (relatively) recent developments that have enabled suppliers to keep pace with the expansion in the hardware base are maintenance processors and remote diagnostics.

A maintenance processor is a separate processor dedicated to the execution of engineering diagnostic programs. More often than not, a maintenance processor can diagnose the cause of the failure in a host processor much more quickly and accurately than can a human engineer. In the future, it is quite possible that a maintenance processor could provide information to allow operations staff to carry out simple corrective procedures, thereby reducing significantly the time required to repair the majority of system faults.

Remote diagnostics is a development of the maintenance processor concept. By providing a communications link between the maintenance processor and a remote engineering site, specialist engineers can diagnose a fault before an engineer is despatched to the customer's site. The engineer therefore usually arrives at the customer's site with the equipment and parts necessary to correct the fault. As a result, the overall time required to correct the fault is reduced considerably. (Remote diagnostics can be used even if there is no separate maintenance processor.)

The need for remote diagnostics becomes greater as distributed system architectures require more processors to be installed in locations remote from urban conurbations. Site engineering support for such locations can be difficult to obtain at short notice.

More resilient system architectures

Resilience in a systems context is defined as the ability of systems to return to normal following an abnormal event. Today's information systems usually operate within a framework or architecture that is much more capable of recovering following an abnormal occurrence than were the typical systems of five years ago. The primary reasons for this change are the increasing use of redundant systems components and the distribution of computing power.

Many organisations build in a degree of redundancy into their processor configurations, and multiple-processor installations are now common. Although all the processors will normally operate in parallel, one of them can act as a backup for the others in the event of a hardware failure. Some suppliers even provide multiple processors as part of their basic hardware architecture (the so-called non-stop computer systems). These systems are being used increasingly for critical processing applications, and they are improving the resilience of many organisations' systems beyond the level that could be attained using conventional processors.

The ability to distribute processing power also provides greater flexibility in the selection of system architectures. Traditionally, a single mainframe system was the only appropriate solution for commercial data processing problems, but today several smaller processors in different locations provide an attractive alternative. A distributed architecture permits the bulk of an organisation's computing workload to carry on as normal even if one part of the overall architecture is totally unservicable.

CHANGING USER ATTITUDES

The technological changes noted in the previous section affect not only the computer services department. They are also responsible for a fundamental shift in users' attitudes towards computer services, and those changes in turn are reflected in the way in which the computer services department fulfils its role. In many respects the changing user attitudes have a more visible impact on the computer services department than the technological changes. In this section we now discuss the two most significant trends that are helping to change users' attitudes — increasing commercial dependence on information systems, and the increasingly critical nature of computer services.

Increasing commercial dependence on information systems

In the early days of commercial data processing, computer hardware was far less reliable than it is now. Information systems users were accustomed to late delivery of outputs caused by hardware failure, or application system problems, or production bottlenecks in the computer room. In the main, these delays did not cause serious problems, because the batch systems supported by the early mainframe installations were not particularly time critical. If the printed outputs from (for example) historically oriented accounting systems or stock control systems were late, the effects were seldom disastrous because these systems were used as audit trails or for verifying records kept manually by the user. As a consequence, most users of traditional batch-oriented systems did not rely solely on the systems' outputs to run their business.

Today, however, information systems users operate in a different environment, and many of them are totally reliant on a timely response from their systems. In addition to the technological changes that we have already discussed (more reliable hardware and more resilient system architectures) this change has been brought about by the evolution of more comprehensive information systems, which can provide their users with most of the required information. As a result, users have learned to trust and rely on the tools provided by the systems; not only have they abandoned their manual backup records, but they now look for additional ways in which new systems can help them.

In addition, the increasing use of online systems is making a broad spectrum of commercial users (including senior managers) aware of application systems that can provide timely and accurate information. There is a growing awareness that such systems can support the day-to-day decision-making process on a real-time basis, thereby providing the organisation with a competitive edge.

Increasingly critical nature of computer services

The increasing dependence on information systems has brought with it a greater appreciation by users of the role that the computer services department plays in providing those services. Historically, most users' attention was focused on the staff who were involved in designing and implementing application systems. Very little attention was given to those who kept the machinery of information systems working. Operations, as it was invariably known, stayed in the background and quietly reacted to the lead provided by the systems development department.

Today, however, organisations are beginning to

realise that computer services has its own leading role to play in the evolution of information systems. Computer services has become a more visible and essential component of the commercial success of the organisation that it serves. If the computer services manager does not do his job properly the effects are felt immediately, and they could be disastrous.

Compare this with a situation where the systems development department is late in delivering a new system, or where a new system does not perform according to expectations. Although each of these events would be highly inconvenient, neither one of them is likely to have a catastrophic effect on the organisation's immediate commercial viability.

Users are becoming more aware of the computer services department for two main reasons:

— Most of the rapid advances in information system technology taking place today are hardware based.

— The systems development department is specialising more and more in the increasingly difficult and time consuming tasks of designing and implementing new, complex application systems and of maintaining existing systems. As a result, users are turning to the computer services department for certain activities previously performed by system development staff.

Hardware-based advances

Most of the major, rapid advances in the information systems industry in the past few years have been based on hardware improvements. The price/performance ratios for hardware systems of all makes and sizes have improved dramatically, and the hardware options available have proliferated. The communications facilities available have also advanced at a rapid pace.

Hardware is increasingly the province of the computer services department. Certainly, new system development methodologies have appeared and these have produced worthwhile benefits. Nevertheless, even the most efficiently managed systems development team using the most advanced methodologies still requires long lead times to produce quality results. The computer services department is able to respond relatively quickly to the problems that it faces because it is dealing with hardware advances that can bring immediate benefits.

Comparisons between the times taken by the computer services and systems development departments to respond to advances in their particular field of expertise are obviously grossly unfair. However, fair or not, corporate management is becoming aware that the computer services function can implement dramatic improvements more quickly than it could in the past. As a consequence, corporate management now perceives computer services as being more critical to the commercial success of the organisation than they once were.

Specialisation of systems development

The nature of the systems development role has become much more demanding during the past five years. The applications being developed today are considerably more difficult than those that were implemented during the early days of commercial data processing.

This is because many organisations are now attempting to automate the more complex aspects of commercial life. The resulting applications require a tremendous development effort, long project durations and an understanding of powerful new development methodologies. Moreover, application systems maintenance is consuming a growing percentage of available resources.

The computing industry is short of people with the necessary conceptual abilities and a background in the new system development methodologies. This shortage has led to a desire by systems development management to deploy their scarce resources in the roles where they are most productive — designing, implementing and maintaining systems. As a result some organisations are transferring some highly visible activities previously performed by systems development staff to the computer services function. Examples include:

— Production system troubleshooting (or a 'helpdesk' facility).

— Application system change management.

— Application package selection and support.

— Operations support programming.

We discuss these activities in more detail later in this chapter. The important point here is that activities such as these increase the visibility of computer services staff to the user community.

CHANGING RESPONSIBILITIES

The responsibilities of, and the range of services provided by, the traditional operations department were relatively straightforward and limited. They fell into the three basic categories of computer operations, data preparation (or data entry) and data control/scheduling. Sometimes, a systems programming function was also part of the operations manager's responsibility.

The responsibilities that typically were assigned to the traditional computer operations department tend now to be concentrated in one section of the computer services department, commonly referred to as pro-

duction or operations. The primary role of this section is to run the operational application systems on a day-to-day basis and to co-ordinate the inputs to and outputs from batch systems. Although the responsibilities are similar to those of the traditional operations function, the number and the type of people required to process a given workload have changed considerably. The personnel issues of computer operations are discussed in chapter 2.

The major changes in the responsibilities of the computer services department have, in fact, occurred in areas not associated directly with operating computer hardware. Many of the computer services organisations we spoke to during the research for this report now have responsibilities in the areas of user support and development support. In the remainder of this section we examine these two areas of responsibility.

User support activities

Some organisations are finding that the computer services department has a wider role to play in providing user support, particularly directed towards production system problems and end-user computing and office systems.

Production systems support

When application system users (particularly online and distributed system users) are confronted with a problem, they often ask the system development staff for assistance. Unfortunately, this procedure is counter-productive for two reasons:

— Many of the production problems experienced with modern systems are not caused by faults in the application programs. More often than not the problem lies within the province of the computer services department (for example, a hardware or communications line failure, or a violation of the operational procedures). When such problems are referred first to the systems development department, valuable time and effort can be wasted before it is determined that the responsibility for resolving the problem lies elsewhere.

— Even if an application program is the cause of the fault, the computer services department is bound to be involved to some extent in resolving the problem, if it is at all serious. Computer services staff should therefore be involved at the earliest opportunity.

One method used successfully by many organisations to counter this problem is to establish a central helpdesk in the computer services department. All production system problems would be referred initially to this helpdesk. It is normally staffed by operations personnel who would be able to diagnose and solve trivial problems. More complex problems would be referred to the appropriate operations analyst. (The role of an operations analyst is discussed in chapter 2.) He in turn would decide if the problem required the involvement of technical support, operations or systems development staff.

The commonly stated advantage of this approach is that systems development staff, who are relatively expensive and often fully committed to development or maintenance work, are not interrupted unless it is absolutely necessary, thus removing one potential cause for the perennial problem of system development project overruns.

End-user computing and office systems support

Various user-driven technologies such as end-user computing and office systems are creating new opportunities for computer services management. But those same technologies are also posing significant challenges. By their very nature, the implementation of user-driven technologies is not planned or closely monitored by management services, and the frequency of their use is unpredictable. In turn, this means that the demand for computing resources also is unpredictable. In such a dynamic environment, capacity planning and resource management can easily degenerate into crisis management, with computer services management merely reacting to user requirements.

One commonly used solution to these problems is to establish a separate end-user support group. (See also Foundation Report No. 30 — End-User Computing.)

The organisational location of the end-user (and office systems) support group is a much debated topic. Powerful arguments can be made for basing the group in the computer services department, in the systems development department, or in a completely separate department. The best solution will depend largely on the organisational structure of, and the existing personnel within, an organisation's information systems (or management services) function, and on the desired orientation of the support group.

Regardless of its organisational position, the group must have an information gathering role for computer services management. If forewarning of new demands for end-user computing resources can be obtained, computer services management has a reasonable chance of having sufficient hardware resources available to meet the demand.

Development support activities

Many systems development support responsibilities have traditionally been performed by the systems development department only because these tasks were considered too technical for the operations staff. Most of the tasks were, in fact, more closely related to the primary responsibility of the computer services

department (providing a stable application systems infrastructure to the user community) than to the activity of building the systems.

But the situation is now changing. Computer services organisations are now beginning to hire and retain more highly qualified personnel who, five years ago, would not have considered operations as a career. As a result, the computer services department is beginning to include higher-calibre staff who can provide services that hitherto were either not provided at all or were the responsibility of the systems development department.

Nearly all of the computer services managers interviewed during the research for this report said that increased participation by computer services staff in systems development projects would improve both the performance of computer services and the quality of the application systems. But, in many organisations, system development project plans still do not require computer services staff to participate until the programming stage or later. At this stage the major design decisions have already been taken, including decisions that will affect the operational characteristics of the system.

One effective approach is for an experienced and qualified computer services representative to participate in the planning and progress review meetings from the feasibility study stage onwards. In this way, the manager of the development project has at his disposal sufficient insight into the practical operational environment to enable him to prevent operations-oriented problems from occurring in the future. Additionally, this approach enables computer services management to be briefed on the progress of development projects which, in turn, enables the computer services department to ensure that sufficient resources are available when needed. The operations analyst is commonly used for this liaison role between the computer services and systems development departments (see chapter 2, page 8).

In addition to providing operations expertise at the development stage, the computer services department is increasingly capable of providing assistance in the areas of production support programming and application package support.

Production support programming

In some installations, a significant proportion of the amendments to operational application systems are related only to the needs of the production department. These changes are usually minor in nature and have no visible effect for the user community. Such changes are frequently given a low priority by the systems development department and, usually, they are implemented with the next set of user-requested amendments. This is unfortunate because many of the long-delayed production support amendments, once made, can contribute significantly to the efficiency of the production department, and therefore of computer services and management services in general.

Some organisations now realise that, provided installation standards are adhered to, these minor amendments could be carried out adequately by a support group within the computer services department. This approach offers two potential advantages:

— Production support amendments will be implemented more quickly and less expensively, thus improving the overall efficiency of the management services department.

— By removing this type of minor maintenance work, the workload of the systems development department is decreased.

This approach, however, has one obvious potential disadvantage. If the work is not performed according to the same installation standards as used by systems development staff, then serious incompatibilities could be introduced into production systems. It would be necessary, therefore, for such work to be supervised by someone who is experienced in using the standards and in system development techniques.

Applications package support

Depending upon the contractual arrangements required by the package supplier, application package support normally requires little technical involvement by the user organisation. Usually, the supplier either maintains the package on an ad hoc basis or provides regular releases of the package. The user organisation needs only to provide a co-ordinating function. This function could be performed quite adequately by computer services staff at less expense than by systems development staff, providing that personnel of sufficiently high calibre and adequate interpersonal skills are available. The requirement is for a mature personality with an understanding of the commercial users' needs and the ability to communicate those needs to the supplier when necessary.

SUMMARY

In this chapter we have focused on the changing (and expanding) nature of the computer services function. In particular, we have highlighted the ways in which computer services is becoming an increasingly critical component of the commercial organisation in its own right.

Not all of the changes identified will be relevant, or even workable, for all organisations. Much depends on the existing corporate culture and on the existing staff within the computer services department.

CHAPTER 2

PERSONNEL ISSUES

In the previous chapter we focused on the changing nature of computer services. The changes identified are having (and will continue to have) a fundamental impact on the nature of the jobs performed by computer services personnel. Some of the traditional jobs are disappearing and new roles (some of which we alluded to in chapter 1) are being created. But, unfortunately, it is not simply a matter of retraining those displaced from the traditional jobs so that they can perform the newly created roles. The new jobs require a different set of personal attributes and skills.

The personnel profile of the typical computer services department is in the process of changing from one that requires mainly unskilled labour to one that requires a smaller number of much more skilled staff. Achieving this transformation is probably the most difficult challenge facing computer services management for the remainder of this decade.

In this chapter we illustrate the magnitude of the problem by examining four types of computer services positions. First, we discuss the declining requirement for traditional computer operators. Second, we examine the specialised new computer services positions that are emerging. Third, we focus on one particular staffing approach — the operations analyst — that several organisations have successfully implemented. Finally, we describe the role of the computer services manager, and the attributes required of the individual who fills this demanding position.

COMPUTER OPERATORS

Traditional computer operators are concerned mainly with the physical aspects of keeping the computer room functioning. They do not require academic qualifications beyond secondary education and they tend to have limited initiative and conceptual abilities. Usually, they do not feel the need to acquire an understanding of the organisation's business.

Because of the various technological changes described in chapter 1, fewer computer operators are now required to process a given workload, and this trend is likely to continue for the foreseeable future. Several of the organisations interviewed during the research for this report were investigating the feasibility of introducing a completely automated operations environment. Some were actually planning to move to an operator-less environment.

As we illustrated in chapter 1, computer services is now a critical component of many organisations' commercial life. It is therefore not surprising that some organisations are seeking ways of automating their computer operations. They cannot afford to be in a position where a small number of computer operators can financially cripple the organisation. A stark reminder of the dangers is provided by the experience of a major public utility in the United Kingdom. A strike by a very small number of operators prevented bills being sent to customers for a period of several months.

In the long term, the trend towards automated operations will undoubtedly have an impact on the number of computer operators required. Computer services managers will have more computer operators than they actually require, and it will not be easy to resolve this problem for the following two reasons:

- Many computer operators' earnings are augmented by extremely attractive shift-work and overtime payments. Their total earnings make it very difficult to redeploy them in other information systems positions, and almost impossible to move them to other clerical positions within the organisation.
- The newly emerging specialised computer positions require skills and attributes that many existing computer operators do not possess (particularly cognitive and conceptual abilities). Even with appropriate training courses, it will be difficult to move such operators to the newer and intellectually more demanding positions.

The computer services manager is therefore left with the difficult human problem of deciding what to do with traditional operators as the requirement for them diminishes. The problem is compounded by the relatively low turnover of operations staff compared with other management services staff.

Few organisations have yet found it necessary to make computer operators redundant, and most organisations have a breathing space in which to consider their responses to the problem, because the widespread use of automated operations will develop only slowly. Many of the older batch systems still operating today cannot be converted or updated and, as a result, the trend towards an operator-less environment will certainly be slow. Nevertheless, we believe that this trend is inevitable, and computer ser-

vices managers should plan now to reduce through natural wastage their requirement for traditional computer operators.

SPECIALIST ROLES

The changing (and expanding) nature of computer services is creating new positions such as operations analyst, technical support specialist and end-user support specialist, and these positions differ from that of the traditional computer operator. To perform these new roles the job holders need to be more technically oriented and to have a greater intellectual ability than the traditional operator. They also require more initiative and the ability to relate more closely to the general business aims of the organisation. Candidates for these roles require higher educational standards than traditional operators, and many graduates would find the positions stimulating and challenging.

The major difference compared with traditional operators is that the emerging specialised roles are far less involved with equipment minding (which implies that the specialist staff will not usually be required to work shifts). Nevertheless, the specialists will still require the ability to resolve operational problems whenever they occur. As systems (both hardware and software) become more reliable, the operational problems will become less frequent, but when they do occur they are likely to be more difficult to resolve. In addition, as organisations become more dependent on reliable computer services, any operational failure becomes critical in nature. Thus, despite the trend towards an operator-less environment, there will always be the need for skilled specialists to step in at short notice to sort out operational problems. The difficulty is that these troubleshooting activities will occupy only a small percentage of the specialists' time, and this raises two fundamental questions:

— How can the specialists be used productively for the larger part of their time, whilst still enabling them to be available at short notice at any time of the day to resolve critical operational problems?

— How should they be organised within the computer services department in order to make the best use of the skilled resource they represent?

There are no all-embracing general answers to these questions. Each organisation needs to work out the specific solution that best fits its own circumstances and corporate culture. The most appropriate approach for the majority of organisations, however, is likely to be based on deploying the individuals concerned in non time-critical but intellectually stimulating positions from which they can be seconded at short notice to resolve immediate operational problems. We have already mentioned several new computer services roles (production support programming, applications package support, end-user support, and so forth) that could provide appropriate positions.

In many respects, the new computer services roles will be more challenging than system development roles because they will require both operations and applications expertise. It may be possible to retrain a few existing computer operators so that they can fulfil the new specialist roles. Some organisations have also found that experienced system development staff can be used for these roles. What is certain, however, is that computer services departments need to review their recruitment policies to ensure that staff of the required calibre will be available to fill the specialist roles.

From the preceding discussion it is clear that we believe that the boundary between computer services and system development responsibilities will become increasingly blurred. As a consequence, there will be greater opportunities for specialists in one of these areas to further their career in the other area.

THE OPERATIONS ANALYST

One example of a relatively new computer services staffing concept is that of the operations analyst. This position is best described as an operations equivalent of a systems analyst. It provides an interface between computer services and the user. (Users in this context also include systems development staff.) In addition, because users will naturally see the operations analyst as their first line of support, the analyst would sometimes provide an interface between the end users and systems development staff.

The primary responsibilities of the operations analyst are:

— To co-ordinate all the elements required for the smooth running of one or more production systems from the time they are implemented.

— To participate in system development projects from their early stages. In this capacity the operations analyst would assist in the planning of machine loadings, data preparation requirements and other operations-related resources essential for operating the system. These activities would be of particular benefit to the capacity-planning activities of computer services management and would provide valuable assistance to systems designers.

— To co-ordinate operations acceptance-testing activities.

— To co-ordinate the creation of the production environment, including the preparation of job control language statements, operations manuals and the definition of backup and recovery procedures.

—To perform first-line fault investigation of production systems and to co-ordinate the specialist expertise necessary to resolve the faults. Specific actions in this context would include correcting data errors and restoring corrupt files. Errors originating in the operating systems, programs or hardware would be referred to the appropriate specialists.

—To co-ordinate the installation of all application system changes generated by systems and programming staff. This change-management function would include verifying that appropriate changes to the operations manual are effected in accordance with the installation standards.

—To monitor the performance of operational application systems, in terms of both operating efficiency and user satisfaction.

Those organisations that have implemented the operations analyst approach believe that the role is vital, especially in large installations. It is also vital to any organisation that has a dynamic, ever-changing systems environment or a large number of remote users.

COMPUTER SERVICES MANAGER

As the demands placed upon the computer services department and the importance of the function increase, the requirements for managing the department change. In particular, the organisation's perception of the role is changing. Previously, the computer services manager was perceived (in naval terms) as a 'chief engineer', who kept the machinery running and responded to demands. Now he is increasingly regarded as a key part of the information systems decision-making process, with a significant contribution to make. The transformation required to meet the challenges of the new role does not happen easily.

The traditional operations manager was typically appointed by promoting an operator or shift leader. More often than not, the appointed manager was given little, if any, additional management training. This approach may have been adequate for the traditional operations environment, but it would leave the manager of a modern computer services department ill-equipped to handle the additional demands that he must now face. These demands arise because the responsibilities of a computer services manager are now much more visible and personally interactive.

To perform his role effectively, the computer services manager needs to be thoroughly aware of impending developments in terms both of systems and of the business as a whole. Insufficient involvement with systems planning and development has been a perennial complaint of operations managers. But it is up to the computer services manager to ensure that his department has the right calibre of staff, and that they are organised in a way which permits them to make an effective contribution to systems planning and development.

Similarly, it is the responsibility of the computer services manager, working with the management services manager, to ensure that other business managers are well aware of the potential contribution that his department can make. It is only by gaining the confidence, trust and respect of his colleagues that he will be able to gain a better understanding of the organisation's likely future needs. Without such an understanding, the computer services manager will not be able to anticipate the demand for increased or changing resources, and he will find himself constantly reacting on an ad hoc basis to the changing needs of the business.

The primary role of the computer services manager is to provide an adequate level of service to the users that he serves. To do this effectively he needs the following skills:

—The ability and desire to understand the business objectives of the organisation that he serves.

—The ability to communicate effectively at all levels with the users. The required levels of service cannot be determined or negotiated unless the manager and the user have a common understanding of the requirements and constraints of the business.

—The ability to respond quickly to changes in required service levels. This demands a sound organisational ability as well as the foresight to be able to predict what the likely changes will be.

—The ability and desire to manage the computer services department as a cost-effective organisation.

—The ability to manage and motivate skilled technical staff who have a variety of skills, backgrounds and abilities.

All these skills have one thing in common. They are general management skills and not technical skills. It is the requirement for man-management and interpersonal skills that distinguishes today's computer services manager from his predecessor, the operations manager.

Nevertheless, the computer services manager must have a good understanding of the operations (production) duties that are part of his portfolio of services, just as his predecessor did. In addition he must also have a basic understanding of his newly added responsibilities — technical support (including data communications), database administration, user support and development support. But, above all, the com-

puter services manager must be a generalist, with good conceptual abilities, and he must be capable of dealing with confidence with the organisation's mainline business managers.

SUMMARY

To discharge its responsibilities adequately, the computer services department must be organised and staffed in a way that is different from that of its predecessor — the traditional operations department. The major change that computer services managers need to come to terms with is that there will be a reducing requirement for the traditional operations role and an increasing requirement for specialist roles in areas such as technical support and end-user computing. The transition will not be easy to achieve. New areas and levels of skills must be effectively managed in addition to many of those that were (and remain) part of the computer operations role.

CHAPTER 3

THE EFFECTIVENESS OF COMPUTER SERVICES

The traditional method of measuring the effectiveness of the computer operations department was to monitor the performance and the utilisation of the hardware employed. This approach is no longer adequate, because the combination of improved hardware price/performance ratios and the constantly increasing cost (and scarcity) of qualified staff is making it essential also to take account of the performance of computer services staff. Although hardware-related factors are still important, they are now a subset of the factors that need to be taken into account when the performance of a modern computer services department is evaluated. The emphasis is no longer on computer performance evaluation, but on evaluating the effectiveness of computer services.

This chapter identifies the key factors that are relevant when measuring the effectiveness of the computer services department. We begin by discussing the objectives and benefits of the computer services evaluation process. We then discuss the prerequisites for a successful evaluation process. Finally, we examine the process itself by describing in some detail a representative evaluation framework consisting of six phases.

OBJECTIVES OF COMPUTER SERVICES PERFORMANCE EVALUATION

The three major objectives of any performance evaluation technique are performance control, performance tuning and performance forecasting.

Performance control is the most basic aim of any performance evaluation methodology. Performance criteria are established for each resource and the actual performance is measured against those criteria. The process of performance control consists of keeping performance within the limits established by the criteria.

In stable conditions, performance control is adequate for most performance evaluation purposes. In reality, however, continual fine tuning of resource performance will be necessary in order to achieve optimum performance in an ever-changing environment.

The final aspect of performance evaluation is performance forecasting, which anticipates the likely effects of changes in workloads or technologies. In the context of computer services the effects of workload increases can be dramatic, and they must be regularly considered.

It is not difficult to relate these three basic objectives to evaluating the operational performance of the hardware aspects of computer services. But computer services performance evaluation should also examine other factors. Thus the evaluation should also examine the quality and relevance of:

—The department's relationships with its hardware suppliers.

—The department's organisational structure.

—Computer services management and personnel.

—Security and safety procedures.

—Standards and operating procedures.

—The department's relationships with its users.

This is only a partial list of the non hardware-related measurement criteria for computer services performance evaluation. An obvious difficulty is that all these criteria are subjective. Nevertheless, an attempt must be made to measure the performance of computer services in each of these areas. For example, the computer services manager must actively solicit feedback from his users, not only to try more closely to match his services to the users' needs, but also to protect himself from unnecessary criticism. Without such a mechanism, the computer services manager may not become aware of user dissatisfaction until some time after the real damage has been done.

BENEFITS OF COMPUTER SERVICES PERFORMANCE EVALUATION

The most obvious benefits of computer services performance evaluation (some of which are apparent from the objectives just described) are summarised below:

—Performance degradation can be identified and, sometimes, prevented.

—A rational basis is provided for making decisions about performance improvements.

—Resources can be utilised more fully and effectively.

—Equipment upgrades can be delayed or avoided.

—Storage media can be used more efficiently.

—Applications systems can become more effective.

—Computer services personnel can be utilised more cost-effectively.

Computer services performance evaluation also has less-obvious benefits which, nevertheless, are just as important as those just listed, especially from the users' viewpoint. Four such benefits are:

—Computer services costs can be reduced when unnecessary resources are eliminated or made available for other purposes.

—The response of the computer services department to users' demands can become more timely because of increased resource capacity.

—The users' perception of the effectiveness of computer services can be improved if performance standards can be made public and consistently achieved.

—The effectiveness of computer services management can be demonstrated by its ability to identify trends and respond to them.

Examples of the benefits resulting from the effective use of computer services performance evaluation are easy to find. One United States government agency invested $60,000 in hardware performance monitoring and, as a result, reduced its annual costs by more than $500,000. This is an extreme example, but it does demonstrate the potential of computer services performance evaluation techniques.

PREREQUISITES FOR AN EVALUATION

Before a computer services performance evaluation can be successfully carried out, three prerequisites need to be satisfied:

—Computer services management must have determined who is qualified to carry out the evaluation in a completely objective manner.

—Service level agreements must have been established between the computer services department and its users.

—The use and relevance of charge-back schemes must have been considered.

Before discussing the mechanics of the evaluation process itself, we first discuss the need for these prerequisites, and the ways in which those needs can be satisfied.

Qualifications and objectivity

Some organisations hire an experienced external consultant who, by definition, has the objectivity necessary to carry out the initial computer service performance evaluation exercise. The exception might be those large organisations whose size warrants a separate in-house team of data processing auditors with the required level of experience and training. Once the evaluation framework has been defined, subsequent evaluation exercises can be performed by suitably qualified employees.

Service level agreements

Stated simply, service level agreements are publicly acknowledged formal agreements between the users of the service and those responsible for providing the service. In the business world, such agreements are commonplace, and they normally take the form of binding contracts between organisations.

In the environment of in-house information systems, service level agreements are a relatively new development. Their format varies from one organisation to another, but the form is not important. The content and meaning of the agreement are the critical factors.

There are four important guidelines relating to the preparation of service level agreements.

Make the agreement jointly

Service level agreements must be established and agreed by representatives from computer services and users. If computer services personnel have the sole responsibility for defining the service level criteria and performance levels, user dissatisfaction is virtually guaranteed. Negotiations between both parties will undoubtedly be required but, if the computer services' representatives approach the negotiations in good faith, agreements can be reached which are acceptable to both parties.

Identify the measurement criteria

Because service level agreements are intended to specify the quantity and/or quality of a service, they must include specific measurement criteria. Each criteria should be stated in terms that describe the level of service acceptable to the user. Examples of these criteria are:

—Response times for online terminal-based systems.

—Frequency for producing printed reports.

—Expertise level of user-support staff.

—The hours during which the service is to be available.

—Minimum reliability of system components, specified in terms of percentages of user working time.

In general, the measurement criteria used should cor-

respond to the criteria established in phase 1 of the computer services evaluation process which is described in the next section.

Formally record the agreement
When the measurement criteria and expected performance levels have been defined, the agreement must be committed to paper for future reference. It is not sufficient for the agreements to be verbal or casual. The lack of a permanent record can easily lead to rancour and unresolvable disagreements.

Regularly review the agreement
The service level agreement must be reviewed regularly both by user management and computer services management so that changes can be incorporated to reflect changing user requirements. A review cycle of six months is recommended.

In summary, service level agreements can provide the computer services manager with excellent reference points against which to measure the performance of his department. Hopefully, he can also use these reference points to measure the rate of improvement in his department's performance.

Charge-back schemes

Discussions about the effectiveness of a service cannot be meaningful unless the agreed level of service is linked to the cost that the user must pay for it. In reality, quality is always related to cost.

The cost of using a computer-based service can be determined either by arbitrarily allocating a fixed overhead cost to a user department or by the use of charge-out or charge-back schemes. The difference between the latter two schemes depends on whether the user actually pays out cash for the services used (charge-back) or is merely told what the service would cost if he had to pay for it (charge-out). For the purposes of this discussion we concentrate on charge-back schemes because they are the more commonly used of the two charging methods. They are also the most meaningful of the three types of approach.

Much has been written about the use of charge-back schemes. We found strong arguments both for and against their use in most of the organisations we talked to during the research for this report. Because of this polarisation of views it is useful to review the rationale for such schemes.

The success of any scheme of this type depends on its compatibility with the organisational culture. First, the scheme must be compatible with the organisation's experience of implementing and using systems. Surprisingly, many organisations are not yet sufficiently mature (in systems terms) for the introduction of charge-back schemes to have anything but a negative effect. In the initial phases of a computer services organisation's existence, the major concern for management is to stimulate and encourage the use of the available services. Cost control measures at this stage could have the wrong psychological impact. This is especially true if the initial users of applications are charged with the entire cost of the computer services organisation merely because of a policy decision that mandates full cost recovery.

Second, the charge-back scheme must be compatible with the organisation's management style. Even the most comprehensive and well thought out charge-back scheme has little hope of success if computer services and user management are not actively concerned about the use of the scheme's facilities. Experience has shown that if computer services management does not ensure that users understand and participate in the scheme, then it will become an expensive overhead, and it will alienate the users.

Provided that these two conditions can be satisfied, charge-back schemes can prove to be a useful element of the mechanism for determining users' satisfaction with the services they receive. But the use of these schemes can also create potential problems for computer services management. Nothing focuses a user's attention more urgently than having to pay the real costs for the services provided.

THE EVALUATION PROCESS

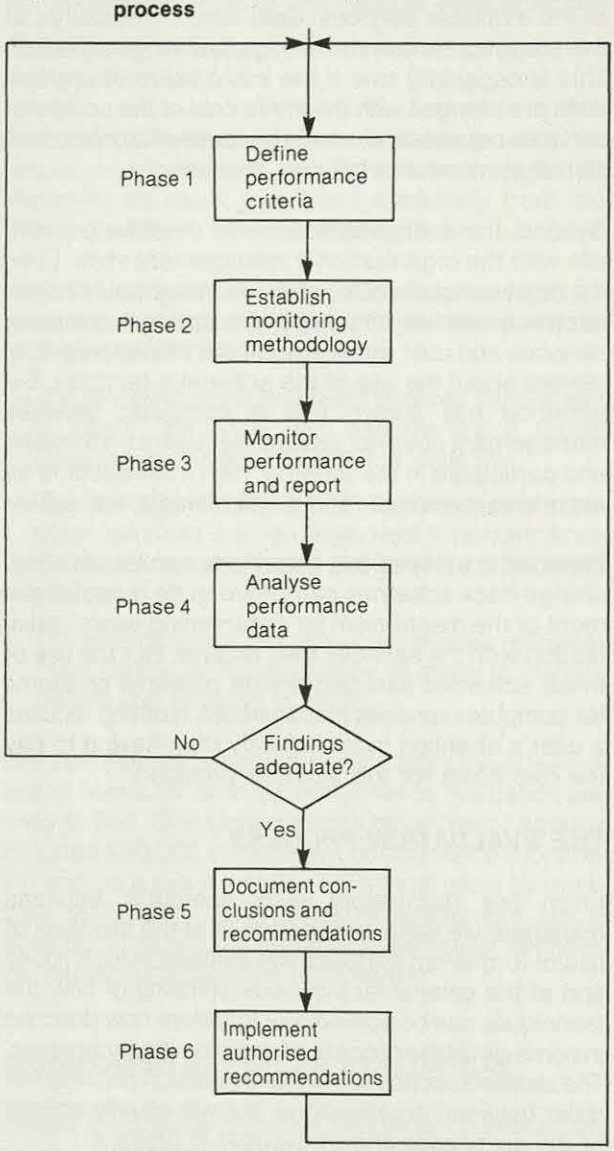
From our discussions with computer services managers we were surprised both at the low level of use of formalised performance evaluation techniques and at the general lack of understanding of how the techniques can be applied. We therefore now describe in some detail the process of applying the techniques. The detailed application of the evaluation process will differ between organisations, but will usually consist of the six phases shown overleaf in figure 1.

The process is usually iterative, with phases 1 to 4 (defining performance criteria, establishing the monitoring methodology, producing performance reports and analysing performance data) repeated at regular intervals. Phases 5 and 6 (documenting the conclusions and recommendations and implementing the recommendations) will be performed at the end of each set of iterations. Although the whole process could be used as a once-off exercise to remedy a known or suspected emergency situation, it is intended to be used on an on-going basis, which should prevent the emergency situations arising.

Phase 1: define performance criteria

A wide range of performance criteria can be used and, often, they are perceived as discrete items with only loose inter-relationships. A better approach is to segment the criteria into the three broad categories of sufficiency, efficiency and effectiveness. These

Figure 1 The computer services performance evaluation process



three categories are related to the functional components of computer services (resources, workload, processes and products), as shown by figure 2.

Sufficiency criteria relate resources to workload. The sufficiency level is determined by whether the available resources are adequate or excessive for the given workload. The availability of resources is a sufficiency criteria, because the apparent inadequacy of the existing resources may in reality be due to the resources not being available.

Efficiency criteria focus on the processing of the workload and on the way in which the available resources are used. These criteria are not concerned with what is processed, but concentrate on how well a particular task is performed. Efficiency criteria are therefore used to measure how well resources are utilised.

Effectiveness criteria are concerned with the users' perceptions of how well the service provided satisfies their needs. These criteria are concerned therefore with what the user achieves as a result of using the service. The effectiveness of computer services can be low even though the efficiency is high, and vice versa. As far as hardware performance is concerned, users will perceive effectiveness in terms of turnaround time or response times. The effectiveness of computer services staff will be perceived in more subjective terms such as the quality of the service provided, how accessible the staff are, how responsive they are to solving immediate problems, the level of expertise they have, the quality of the training and guidance they provide to users, and so forth.

Phase 2: establish monitoring methodology

In order to monitor the performance of the computer services organisation, considerable amounts of data must be gathered about the various components of the organisation, and in particular from the hardware itself. One approach to the formidable task of gathering such data has been suggested by IBM as a result of a performance study carried out in the management information division of the State of Illinois. This approach segments the computer configuration into six functional subsystems, each with its own performance criteria, as summarised in figure 3. The figure also lists the three types of variable factors (controllable, uncontrollable and catastrophic) that will

Figure 2 Relationships between evaluation criteria and functional components

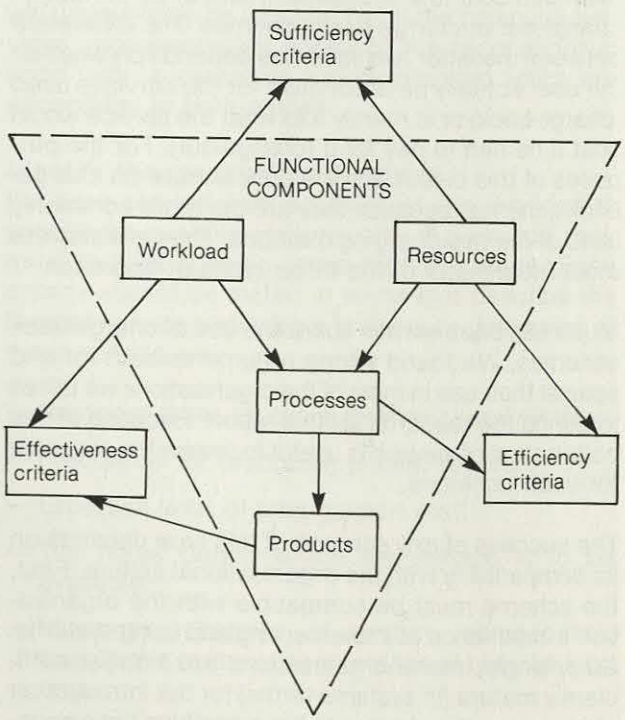


Figure 3 Performance evaluation subsystems, criteria and variables

Subsystem	*Criteria*	*Variables*		
		Controllable	*Uncontrollable*	*Catastrophic*
Remote I/O	Channel utilisation	Terminals per line Terminal types Numbers of lines Line types Numbers of transmission control units	Terminal down Line or modem down Line quality	Channel down Transmission control unit down
Remote request	Response time Transactions per time unit Time last request processed		Monthly fluctuations Weekly fluctuations Daily fluctuations Hourly fluctuations Programmer attendance Software status	Agency conditions
Operations support			Request time delay Number of operator errors Number of operators	Operator error
CPU	CPU utilisation Average time transactions in queue Average number of transactions in queue	SYSGEN options PARMLIB options Number of initiators Same subsystem tasks Same core allocation	Operator actions	CPU down
Local I/O	EXCP count Channel utilisation	Hardware configuration Volume configuration Library placement	Devices unavailable Sharing devices Error recovery	Hardware failure
Job submittal (Batch/RJE)	Turnaround time Throughput Backlog size Job queue averages		Monthly fluctuations Weekly fluctuations Daily fluctuations Hourly fluctuations Programmer attendance Software status	Agency conditions

(Source: IBM Manual 6320-1373-0; Study Results: State of Illinois, Data Security and Data Processing)

affect the performance criteria measurement results. The factors listed were specific to the particular installation studied by IBM, and they may not all be relevant for other installations.

Segmenting the configuration in this way provides two benefits. It increases the likelihood of thorough and systematic data gathering, and it provides a convenient structure for analysing performance and for reporting conclusions.

The required data for hardware performance can be gathered by a variety of methods, ranging from sophisticated modelling and simulation techniques to hardware and software-based monitors. At present, monitors are more widely used than the other methods. A monitor collects performance data from the computer system as the workload is executed, and so the accuracy of the data gathered does not rely on guesswork or estimation, as it might with modelling or simulation techniques.

Although the examples quoted relate specifically to the hardware component of the computer services organisation, the same principles apply for gathering information about other computer services resources. One important point to remember is that it is only worthwhile collecting data that is going to be useful. Thus, the data collection procedures should concentrate on those areas that are likely to be candidates for improvement.

Phase 3: produce performance reports

In those installations successfully using performance evaluation techniques, the performance reports usually correspond to the three types of performance criteria defined in phase 1.

For example, hardware resource sufficiency reports would identify how much of the available computer time was used and what it was used for. By compiling such reports at regular intervals and comparing successive reports, specific sufficiency trends may become apparent. In this way, the origin of a potential problem may be observed, and corrective action can be taken before the problem becomes critical.

Staff effectiveness reports could be generated by comparing the level of staff support (from an end-user support team, for instance) promised in a service level agreement with the users' subjective opinion of the actual quality of the support received. By soliciting the opinions of a variety of users, a reasonably accurate picture can be formed of the effectiveness of the user-support.

Resource efficiency reports would typically provide information about how much of a resource was used productively. By obtaining information about items such as processor idle time, the number of re-runs, operator error rate, etc., one can assess how efficiently the computer services resources are being used.

Phase 4: analyse performance data

There is no general-purpose methodology available for analysing the performance reports produced during phase 3. The following guidelines can be used, however:

- Tackle the obvious problems first. Attention must first be focused on the clearly defined, high-priority problems. More complex problems usually require complex, time-consuming solutions.
- Study only those improvements that can actually be implemented.
- Consider the inter-relationships between the problems. Beware of solving one problem and creating a worse problem in another area.
- Observe long-term performance trends. Performance evaluation techniques can generate a vast quantity of detailed day-to-day data. Long-term trends should be extrapolated from this data.

The results of the analysis may be inconclusive, in which case phases 1 and 2 should be re-examined to determine if the performance criteria and monitoring methodology are adequate.

Phase 5: document conclusions and recommendations

Again, no general-purpose methodology is available, but the following guidelines have been found to be helpful:

- Reports to management should be as concise as possible, clearly written and unambiguous.
- Performance evaluation reports should be prepared on a regular basis. Monthly or quarterly is usual for hardware-related reports. Performance reports relating to personnel performance tend to be produced on a six-monthly or yearly basis.
- Detailed evidence must be available to support the conclusions and recommendations made to management.

In many respects, the conclusions and recommendations from performance evaluation exercises should be presented in the same way as the results of conventional cost-benefit analyses. This procedure consists of four elements:

- Stating the alternative approaches.
- Stating the costs that would be incurred to implement each approach, together with the costs of not implementing any of them.

—Stating the benefits that would accrue from implementing each approach.

—Recommending the preferred approach.

Phase 6: implement recommendations

Once the recommendations made in phase 5 have been accepted and approved, it is usually a straightforward and short-term activity to implement them. The required changes usually involve adding, removing or modifying resources. One point to remember, however, is that implementing significant hardware or software changes will almost certainly affect the criteria and methodology for subsequent computer services performance evaluation cycles.

SUMMARY

Those organisations that utilise some type of formalised process for evaluating the performance of their computer services departments usually find that the process pays for itself in the long term. The pay-back normally comes in two ways:

—The overall performance of the department is improved.

—The reputation of the department is enhanced because it is seen to be a concerned part of the commercial organisation willing to submit itself to a process of self-examination.

The real measure of computer services effectiveness is no longer determined merely by analysing the performance of hardware. Today's users are demanding satisfactory performance at competitive costs. If the existing computer services management cannot provide satisfactory services, other people, or organisations, will.

CHAPTER 4

INTEGRITY OF COMPUTER SERVICES

As organisations become increasingly dependent on computer-based services, management is becoming more concerned about the potential impacts both of interruptions to the services and of unauthorised use of them. The potential threats to the integrity of computer services are increasing in direct proportion to the increased importance and complexity of those services.

Much of the responsibility for ensuring the integrity of computer-based systems falls on computer services management which, in some organisations, is responding admirably to the challenges presented by these issues. This is particularly true for financial institutions, where security has always been of paramount importance. Nevertheless, our research revealed disturbing and widespread lack of knowledge and concern about the increasing significance of systems integrity. It is for this reason that we present in this chapter an overview of the most important aspects of systems integrity as it applies to computer services.

We begin by reviewing the risks that can threaten the integrity of computer services and then we identify the potential losses that can result from the most conspicuous risk — a data centre disaster. Next we describe the essential elements of a risk-control programme. Such a programme can never guarantee that a disaster will not occur and so, finally, we provide guidelines for preparing a contingency plan for recovering from a data centre disaster.

THE RISKS

In the computer services environment threatening events occur infrequently, but when they happen their consequences can be very costly. The events that can pose a significant threat can take many forms, some of which might not appear at first sight to warrant concern.

The most common types of threat to the integrity of computer services are:

— Unauthorised access to information and physical installations.

— Physical damage to premises and equipment.

— Loss of essential services.

We now describe each of these in turn. The list of items is not comprehensive, but it does highlight the nature and scope of the threats that computer services management must be aware of.

Unauthorised access to information and physical installations

As the commercial information system user becomes more dependent upon his systems, the amount of sensitive information stored in these systems increases. If this information falls into the wrong hands (either inside or outside the organisation) undesirable consequences can result, ranging in severity from the merely embarrassing to the disastrous.

This problem is prompting an increased interest in two means of protecting information:

— By restricting physical access to the computer facilities and stored information. This usually takes the form of increased security procedures, electronic locks on doors and secure storage of sensitive printed outputs. We were pleased to find that most of the organisations contacted during the research for this report had implemented suitable access controls to protect their physical installations.

— By restricting access to terminal-based information systems. This is more difficult to achieve than restricting physical access. Most online systems utilise some form of privileged access through passwords, but such controls are only as secure as the individual users who know the passwords.

A second approach to providing access control is to use system-wide access-control software which is application independent. Many packages of this type are available and, when implemented properly, they can be a useful access-control tool. Unfortunately such tools are available almost exclusively for mainframe systems. The minicomputer components of many distributed information systems cannot always make use of them.

Physical damage to premises and equipment

Fire is the threat that most computer services managers think of first when they consider potential disasters. Organisations with centralised computer facilities are particularly vulnerable to fire and the effects of the resulting smoke and corrosive fumes. Fire can cause permanent damage to equipment and stored information in a very short period of time.

Equally crippling damage can be inflicted by smoke and fumes in an even shorter time, without flames actually reaching the equipment.

Water damage is the second most common type of potential risk to premises or equipment. This type of risk can, of course, be eliminated by locating the facility in an area that is not subject to flooding or leakage from internal plumbing.

A third potential cause of physical damage is vandalism or terrorist attacks, and it is a disturbing fact of life that both of these forms of violence have increased dramatically during recent years, particularly in Europe. Modern data centres are very vulnerable to such threats, especially from a determined and often well-trained and equipped terrorist.

Usually (but not exclusively) the threat posed by vandals and terrorists takes the form of fire and explosion. But it is not unknown for a disgruntled employee to cause considerable damage to a data centre by intentionally destroying (or modifying) critical information or software stored in a computer system. Given a sufficient level of expertise and the opportunity, such a person can cause an enormous amount of damage, damage which often remains undetected for a long time.

Loss of essential services

This type of threat can take a variety of forms, any one of which could have significant consequences for the supply of computer services. The three most common threats concern the electrical supply, the air conditioning and telecommunications facilities.

Interruption or fluctuation of electrical supply
The most effective (and the most expensive) means of defence against interruptions or fluctuations in the electrical supply is to use an uninterruptable power supply. Such a supply will normally provide power for a short period of time to selected equipment from a combined battery and dc-to-ac inverter.

Loss of air conditioning
The effects of a breakdown in the air conditioning are often neglected when organisations consider the various threats that face computer services. But a failure in the air conditioning plant can shut down critical computer services just as effectively as can a malfunction in a mainframe processor. In addition, an air conditioning system often takes longer to repair.

Loss of telecommunications facilities
A breakdown in externally supplied telecommunication facilities is a particularly difficult problem. The effects of such an occurrence can be just as serious as a computer malfunction, particularly to remote online system users. The problem is compounded in that preventing, diagnosing and repairing such breakdowns is completely out of the hands of the computer services manager.

The only effective defence against this type of threat is to duplicate the telecommunication lines that come into the data centre, preferably with each line coming from a different exchange. This is obviously expensive but, for users who are increasingly dependent on systems provided via telecommunication facilities, it may well be a viable option.

THE POTENTIAL LOSSES

We now turn to the potential losses that an organisation could suffer if the threats identified in the previous section actually occur. We concentrate on the potential impacts of breaches in physical security because these most graphically illustrate the potential commercial losses that could arise. The losses can be categorised in several ways, but we have chosen to group them under four headings — direct financial losses, indirect financial losses, loss of control and embarrassment to the organisation.

Direct financial losses

The most immediate and obvious consequences of an interruption in computer services are direct financial losses. Most companies would expect any losses to their computing equipment and facilities caused by a disaster to be covered by their fire and accident insurance. Many companies, however, keep no permanent and up-to-date record (held, of course, in a safe place) of all the relevant items, together with their serial numbers, purchase dates, and values. Insurance claims may therefore prove to be contentious. Furthermore, insurance may cover total destruction but not partial damage (such as that caused by smoke) which does not ruin the equipment completely, but which does necessitate expensive repairs. Some equipment may be impossible to replace because the manufacturer has gone out of business.

A recurring problem in computer insurance today is whether the policy covers the original cost of older equipment, or only the current cost of a new equivalent replacement, which may be much less expensive.

For many organisations, however, the largest direct financial losses resulting from a computer disaster would be from loss of sales or from loss of production.

Loss of sales
Without the assistance of their computer systems at some stage of the process, many organisations would today find it very difficult to sell their products or services. This threat is most severe with systems that are strongly transaction-oriented. For example, order-taking by telephone is frequently supported by termi-

nal-based online order-recording systems, sometimes with no alternative manual means of input. In such systems, orders can be loaded into the system only through a computer terminal.

Loss of production
Many companies have invested immense effort in computerising their production processes to some degree. In some industries, the production line is linked to the mainframe computer (often through an intermediate process-control computer), and cannot function properly without access to the computer's files of production orders or inventory levels.

Although this arrangement may prove beneficial to the company in terms of economy, speed, and quality control, it also makes the production line dependent upon the computer being constantly available. If the computer is out of service, the production line may come to a halt.

Indirect financial losses

If an organisation's computer is out of action for a prolonged period, indirect financial losses are likely to result. These losses can be very difficult to foresee but, nevertheless, they can be very serious. They can arise in several forms, including long-term loss of customers, extra payments to staff, uncollected receivables, undetected fraud and payment of fines or penalties.

Long-term loss of customers
A prolonged computer breakdown is likely to lead eventually to a reduced or degraded service to customers. The speed with which the impact would be felt depends very much on the type of industry. For example, an airline's or a bank's customers would immediately be aware of the effects. On the other hand, a car manufacturer's customers might not notice any reduction in service until much later.

If the interruption to computer services proves to be a lengthy one, or the inconveniences particularly annoying, then some customers will take their business elsewhere, usually to a direct competitor.

Extra payments to staff
Information systems have enabled organisations to reduce the number of staff employed in many clerical departments. If all computer support were suddenly removed for a prolonged period, the business would have to try to cope with its normal clerical workload using purely manual methods. Many organisations would be surprised to discover that they could not now cope with the workload (even though they were able to cope in the past) because there are no longer enough staff to do all the work manually.

It would then be necessary to bring in (or divert) large numbers of clerical staff to do work such as recording orders, preparing invoices, maintaining ledgers, etc., until the computer system was fully restored. One way or another, these extra staff must be paid for.

Uncollected receivables
Processing debtors' ledgers and other receivables is an important application in most computer systems. If the flow of funds is interrupted or slowed down because of a computer disaster, extra bank loans might be needed in order to obtain additional operating capital.

Undetected fraud
The period immediately after a disaster can be a confused and chaotic time for an organisation. Many manual and computerised checks and safeguards, carefully built into the firm's operating procedures, may have to be temporarily abandoned or bypassed in order to get essential work done on time. Unfamiliar faces may be present in the building to help clear backlogs of work. Security measures are fully stretched, and it is an ideal time for many kinds of fraud on the part of employees, customers, suppliers, and others. Unfortunately, there are always some people who will take advantage of a company's misfortunes and temporary vulnerability for their own dishonest ends. It may be a very long time before the effects of their actions are discovered.

Payment of fines or penalties
Not being able to access or process computer records may mean that important deadlines for payments are inadvertently missed. The most visible event would be for the organisation to fail to meet its payroll obligations, thereby severely testing the loyalty of its staff. Other missed payments (for contracts, tax instalments, etc.) may mean that the company incurs financial penalties or fines for being late.

Loss of control

Many managers fear that their increasing dependence on computer systems means that they have less direct control over vital aspects of the business. Paradoxically, the loss of control would be even greater in the event of a computer disaster, because a system's basic controls and safeguards might well be bypassed in an attempt to mitigate the effects of the disaster. Any data subsequently entered into the system must be treated with doubt and suspicion until the system has been fully restored and validated. Management cannot have full confidence in the data's validity or accuracy if the full range of system checks has not been performed. Even if data errors are known to have entered the system, it may not be possible to identify and amend them promptly.

Embarrassment to the organisation

A computer disaster can have long-term effects that

can severely embarrass the organisation and that are impossible to rectify after the event. They normally come about because the company's public image is adversely affected.

The news media in some countries still maintain an ignorant and suspicious view of computers, and rarely pass up an opportunity to publish lurid accounts of computer failures that often bear little resemblance to the truth. It is all too easy for a disaster at a computer centre to result in a dramatic media exposure of unfortunate or compromising events, thus giving an undesirable and perhaps completely inaccurate emphasis to the incident. This may lead to the public perceiving the company as an unreliable, poorly planned and badly controlled organisation — a description that may be all too accurate, at least as far as its contingency planning is concerned.

RISK CONTROL

In the context of information systems, risk control ensures that all assets (hardware, software and data) are protected against accidental damage or unauthorised access. In reality, absolute security is impossible. Nevertheless, applying a properly designed and managed risk-control programme can provide an acceptable level of protection. It is impossible to devise a single risk-control programme that is suitable for all circumstances. But it is possible to describe the general conceptual guidelines that are now being used in this field.

The risk-control programme should be viewed as part of an on-going risk-control cycle that is designed constantly to monitor and improve the programme in response to changes in the information systems environment. Typically, there are four phases in a risk-control cycle:

— Establishing risk-control guidelines.

— Performing a risk analysis.

— Implementing the risk-control programme.

— Monitoring and evaluating the programme.

Establishing risk-control guidelines

Responsibility for the risk-control programme must be clearly established before beginning the cycle. Usually, one person is assigned to this task on either a part-time or a full-time basis, but in some large organisations two or more people may be assigned full-time. The responsibility is often assigned to the person who is responsible for monitoring computer services effectiveness, usually reporting directly to the computer services manager in a staff advisory position rather than line management.

We believe that this approach is particularly effective for two reasons:

— Removing the responsibility for the risk-control programme from the line-management structure allows an objective risk assessment of all functional areas associated with computer services.

— Delegating the responsibility ensures that the computer services manager does not neglect the programme and treat is as a low-priority item. Many computer services managers find that they never actually implement and monitor a risk-control programme themselves, because their other pressing duties leave little time for thinking about an issue that has not yet become a crisis.

Once designated, the responsible person must define the guidelines necessary to ensure that the risk-control programme is effective for the specific organisation. The guidelines consist of standards and procedures for documenting each phase of the risk-control cycle. For each task of each phase, four items need to be documented:

— The objective of the task.

— The responsibility for carrying out the task.

— The timescale for performing the task.

— The method to be used for performing the task.

Many computer service organisations have found that preprinted forms are helpful for documenting these items, particularly in phases 2 (risk analysis) and 4 (monitoring and evaluation). Special legal, political or financial constraints that are pertinent to defining the level of risk should also be documented.

Performing a risk analysis

Risk analysis identifies, assesses and selects the risks to be controlled. The potential risks as far as computer services management is concerned were discussed earlier in this chapter. The specific risks for a particular organisation can be identified only by a thorough and objective examination of the organisation's computer services environment. The need for objectivity in this process cannot be over-stressed.

Once the potential risks have been identified, the next step is to assess their potential impact on the organisation. The impact of each risk can be assessed by estimating the probability of the risk occurring and the financial consequences. The risks can then be ranked according to their relative impacts. Alternatively, many computer services managers prefer to rely on their intuitive judgement when ranking the severity of the risks.

Implementing the risk-control programme

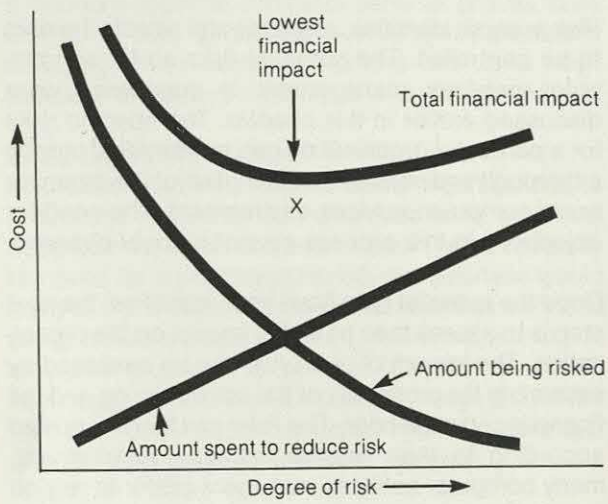
The risks identified during the risk-analysis phase can be divided into two categories. The first category includes those risks that the organisation will accept in their present form. The decision to include risks in this category usually results either from the low potential impact of the risk, or from the high cost of preventing it occurring.

A report published by IBM Sweden examined the relationship between risk-control costs and the exposure to risk. Figure 4 depicts the findings of their study. As the amount spent on risk control increases, so the organisation's exposure to loss is reduced. But beyond a certain level of expenditure (shown as point X in figure 4), the overall financial impact begins to increase again. The conclusion is that each organisation must determine how far to go in risk control. This inevitably means that an organisation has to accept that, in financial terms, it is not worthwhile taking steps to prevent some of the risks occurring.

The second category of risks identified during the risk-analysis phase consists of those that require attention. One or more of the following five types of action may be necessary:

—Transfer the risk. Severe risks that are either impossible or too costly to prevent may be transferred to another organisation through some form of insurance. Various types of data centre insurance are available, ranging from replacement of hardware to reimbursement of the costs of reproducing data. The premium rates for any of these types of insurance can be reduced when adequate protection measures exist. Indeed, some forms of insurance may be impossible to obtain unless such protective measures have been taken.

Figure 4 Costs and benefits of risk control



(Source: IBM Sweden)

—Prevent the risk occurring. Insuring against a risk is the last line of defence. Preventing the risk occurring is the first line of defence. Much has been written on this topic, but for the purpose of this report it is sufficient to say that each of the potential risks identified in the risk-analysis phase must be analysed and an attempt made to develop means of preventing them occurring.

—Define procedures for detecting breaches of security. However thorough the security procedures are, it will still be possible for threatening events to occur. The second line of defence is an effective detection mechanism. Usually, this involves a passive monitoring system, and a procedure for responding rapidly to breaches of security once they have been detected. But, in our view, a passive monitoring system is not sufficient in today's highly complex computer services environment. What is required is an active system for testing the security procedures that will detect any weaknesses in the procedures.

—Plan to respond quickly. The effects of a threatening occurrence can be minimised by ensuring that possible risks are detected quickly, and that prompt corrective action is taken.

—Define contingency plans. Some risks cannot be eliminated completely, and contingency plans for recovering from a data centre disaster should be defined. This topic is discussed below.

Monitoring and evaluating the programme

Once the risk-control programme has been implemented it must be reviewed regularly to ensure that it takes account of any changes in the processing environment. Such reviews usually include random tests of the programme procedures. Any changes required in the procedures should be implemented as quickly as possible.

CONTINGENCY PLANS

In the context of computer services, the most important aim of contingency planning is to enable an organisation to recover successfully from a major data centre disaster such as a flood or fire. Any such contingency plan must provide sufficient reliable backup resources to permit the organisation's key information systems to continue to operate, perhaps at a reduced level of service. The backup resources required by an individual organisation can be determined only by an in-depth study of the processing environment and workload. Many different approaches can be taken for providing backup resources, ranging from a 'warm' standby installation which duplicates the resources, to a share in what are termed empty shell facilities. Figure 5 summarises the various approaches and figure 6 contains a checklist of ques-

Figure 5 The approaches to computer backup

Approach	*Advantages*	*Disadvantages*
Do nothing	Very low cost	Great exposure to risk
'Fortress' computer centre	Relatively low cost Ease of control Good security possible	Exposure to risk (no backup)
'Cold' backup service	Low cost Separate security system	Timescale for recovery Restrictive agreements Shared membership Possible under-capacity
Portable backup centre	Simplicity Low cost Space-saving	Often useless in urban areas Need for special environment Delays in obtaining equipment Poor security
'Warm' backup service	Short timescale to recovery Good environment Good security	High cost Restrictiveness of sharing Possible incompatibility Need for special arrangements
Mutual backup arrangement	Very low cost Good reliability, security	Need to find suitable partner Legal and contractual difficulties Capacity and compatibility may alter with time
Private 'cold' backup centre	Guaranteed access Low cost Flexibility of use	Timescale for recovery
Private 'warm' backup centre	Short timescale for recovery Alternative uses of centre Reliability	Very high costs Difficulties of control and synchronisation

(Source: Computer Disasters and Contingency Planning, Amdahl (UK) Ltd.)

tions that need to be asked about a potential backup computer installation.

There are four minimum requirements for a properly prepared contingency plan:

—The plan must be documented and distributed to everybody who may be affected by a data centre disaster, including key user personnel.

—The responsibilities for carrying out the tasks needed to implement the contingency plan must be clearly identified.

—The plan must be reviewed at frequent intervals, so that it can be modified to account for any changes in the processing environment.

—The plan must be tested regularly to ensure that it works.

These are the minimum requirements for an adequate contingency plan. Other items would be added according to individual circumstances. The aim is to describe clearly how to use the backup resources, and to ensure that all those who might be affected by a data centre disaster know precisely what they have to do.

Figure 6 Checklist of questions relating to a backup computer

1. Is there a backup computer available (either your company's own or someone else's)?
2. Do you have guaranteed access to it in the event of an emergency?
3. Is it periodically 'sized' to ensure its capacity and compatability with the main computer?
4. Are copies of computer files stored at or near the backup site?
5. Are these files regularly tested for their contents and completeness?
6. Are production programs regularly tested on the backup computer?
7. Are staff at the backup site experienced in running the company's main application programs?
8. Are stocks of the company's standard forms and stationery kept at the backup site?
9. Can telecommunications easily be switched to the backup computer?
10. Is there room at the backup site for people from the main centre to work?

(Source: Computer Disaster and Contingency Planning, Amdahl (UK) Ltd.)

During the research for this report we discovered widespread deficiencies in two particular areas of computer services departments' contingency plans:

—The majority of computer services organisations have not established a contingency plan that sets out a detailed recovery procedure.

—Many organisations are depending on computer backup arrangements that are inadequate for the processing environment in which they now operate.

Both of these deficiencies have the same root causes: either computer services management cannot devote enough time to preparing contingency plans, or management in general is not aware of the potential consequences of a major data centre disaster.

We strongly advise such organisations to follow the example of some of those we interviewed. These organisations had recognised the changing requirements for disaster recovery procedures and were responding accordingly, although a few of them were taking excessive precautions that could not be justified in terms of the risks eliminated.

Our research showed that the subject of computer services contingency planning is still relegated to a secondary position behind the day-to-day business of getting the primary job done. As one data centre manager remarked to us: "Our current informal approach has been used for years and has not even been put to the test. What is there now to cause us to change?"

Perhaps nothing has changed. Perhaps the existing approach would work if it was tested. But perhaps a more formal approach would remove the need to ask the question.

SUMMARY

In this chapter we have presented an overview of the key issues relating to the integrity of modern systems. We have shown that the consequences of a disaster affecting an organisation's computer services can have profound and wide-ranging implications. The underlying message is that the criteria and mechanisms needed today to measure and control the integrity of information systems are not necessarily the same as those that were satisfactory five or ten years ago. Users are demanding much more from modern information systems both in terms of performance and of integrity. In order to ensure that the systems measure up to the users' increasingly stringent requirements, the mechanisms used to measure and control systems' integrity must be adapted accordingly.

CHAPTER 5

GUIDELINES FOR COMPUTER SERVICES MANAGEMENT

In the preceding chapters we have discussed the key issues for managing operational computer services in today's changing information systems environment. In this final chapter we summarise the primary lessons that we have drawn from our research by presenting a series of guidelines that computer services managers can use as they face the challenges presented by this changing environment.

These guidelines are not meant to provide a complete textbook on how to manage operational computer services. Rather, they are intended to provide the experienced computer services manager with ideas upon which he can focus his attention as he adapts to the changing role of his department.

PREPARE FOR A CHANGING COMPUTER SERVICES ENVIRONMENT

Chapter 1 emphasised the changing nature of computer services. Computer services managers must prepare themselves, their departments and their organisations for the dramatic changes that are occurring, and will continue to occur for the remainder of the decade. The changes will occur in four main areas:

—Computer operations techniques.

—Telecommunications.

—System architectures.

—New support roles.

Computer operations techniques

Computer services managers must recognise the growing trend towards automated operations and plan to respond appropriately to the challenges that this change will bring. In particular, the computer services manager must determine:

—The availability of automated operations tools for the specific hardware and systems software environment, and the best method for utilising them.

—The best method for eliminating those traditional operations staff positions that will no longer be required, and for redeploying the displaced staff in a sensitive manner with the minimum of disruption.

—The most appropriate means for recruiting, organising and managing the staff who will fill the highly technical and intellectually demanding operations positions that will emerge. Unfortunately, the job gains in these areas will not match the job losses in the traditional operations area, and not all of the displaced staff will be candidates for retraining.

Once policies for each of these issues have been determined, the resulting procedures will take time to implement. Organisations should therefore not delay before addressing these issues, even though some of them may not seem to be of immediate relevance. We believe that sooner or later all organisations will have to face up to these issues. It is better to do so now, rather than wait until circumstances force the pace. A properly planned programme for change will cause far less disruption in the long run.

Telecommunications

An understanding of the concepts of data communications is now essential for the successful computer services manager. Without a sound grasp of the principles of the emerging technologies it is easy to become confused by the plethora of competing (and often conflicting) alternative communications techniques. The computer services manager should be in a position to play a leading role in advising senior management which of the many alternatives is most appropriate for the organisation, its business and its future plans.

In the medium to long-term future, computer services managers in many organisations will have the opportunity to contribute to, and in some cases to lead, the plans for migrating to an integrated voice and data networking infrastructure. Ultimately, integrated networks will be based on digital transmission techniques, but in the interim period analogue techniques will remain important both for voice and for data communications. If the computer services manager wishes to contribute to the plans for an integrated network service, he would be well advised to gain an understanding of analogue transmission techniques.

System architectures

The current trend towards distributed processing and online systems will continue for the foreseeable future. The implementation of these systems will continue to have a significant impact on the demands placed on the computer services manager. If he has not already done so, now is the time for the computer

services manager to become thoroughly familiar with the concepts of these new architectures. Without such an understanding he will not be able to play an active role in helping his organisation to use these tools, and he will be restricted to reacting to them when they are introduced by someone else.

New support roles

Today's computer services manager is increasingly presented with the opportunity to assume responsibility for new support functions such as end-user support and systems development support. Providing and managing these support roles require a different set of skills from those possessed by the traditional computer operations staff member or manager. It may not be readily apparent that, organisationally, the computer services department is the most appropriate group to assume these new roles. Thus, to enable the department to achieve its full potential the computer services manager must:

- Recognise the opportunities for assuming these responsibilities and demonstrate to senior management the advantages to the organisation of assigning them to the computer services department.
- Develop the expertise required within his department to discharge successfully these responsibilities.
- Determine the computer services organisational structure that is most suited to managing the new responsibilities in parallel with existing responsibilities, and prepare to implement the appropriate changes.

Particular attention should be paid to developing the interpersonal communications skills of those staff who will perform user or systems development liaison roles.

IMPLEMENT A CONTINUING EVALUATION PROCESS

The 'ideal' operations department of ten years ago would be totally inappropriate today, and the 'ideal' computer services organisation of today will almost certainly be totally inappropriate in ten years' time. In order to ensure that the services provided continue to meet the needs of the organisation, the computer services manager must have a means of evaluating on a continual basis the quality and the suitability of the services. Implementing such an evaluation process requires that the computer services manager:

- Understands the real needs of the business.
- Regularly re-appraises the effectiveness of the services.

Understand the real needs of the business

Before the computer services manager can evaluate how well the services he provides match the requirements of the organisation, he must first ensure that he fully understands the nature, scope and long-term plans of the business. The most effective means of obtaining this understanding is to ensure that senior management is made aware of the potentially powerful resource that computer services represents — provided it is given the time to prepare itself for the future needs of the business. As this awareness grows, there will be more opportunities for computer services management to participate in the main stream of business life which, in turn, will lead to a better understanding of the evolving needs of the business.

The responsibility for making senior management aware of the potential can fall only on the computer services manager himself. He must understand fully the mechanics of the organisation's business, and he must demonstrate this first to his immediate superiors and then, through them, to senior management. It is clearly important that all levels of information systems management work in concert towards this end.

Regularly re-appraise the effectiveness of the services

Armed with a sound understanding of the mechanics of the organisation, the computer services manager, working with and through users and other information systems personnel, should regularly re-appraise the effectiveness of the services. During each re-appraisal, six key areas should be examined:

- How well does the nature and the quality of the service match the needs of the business?
- Is the relationship between the computer services function and the user community (including systems development staff) one of mutual respect and co-operation?
- Does the user community feel that it receives value for money?
- Is the best use made of recent technological and methodological advances?
- How effectively are the available resources (including human resources) used?
- Does the integrity of the services match the characteristics of the business?

A negative answer to any of these questions will identify an area for improvement. But to answer these questions objectively is very difficult, particularly for someone who is working in the area being appraised. Some organisations overcome this difficulty by employing an independent, outside observer.

In chapter 3 we pointed out that, in addition to objectivity, the essential prerequisites for a successful evaluation process are service level agreements and

charge-back schemes. Service level agreements are a vital ingredient for measuring the effectiveness of computer services. Charge-back schemes should be implemented wherever possible to allow an accurate assessment of the cost-effectiveness of the service to be made. Arbitrarily allocating the cost of computer services as an internal overhead charge should be restricted to organisations in the early stages of implementing very costly facilities that eventually will be shared by many users. Early users of such a facility should not be expected to bear an unrealistically high cost merely because they are the pioneers.

IMPLEMENT A RISK-CONTROL PROGRAMME

We believe that until he has implemented a formal risk-control programme, the computer services manager cannot state with confidence that the integrity of the services provided is sufficient for the needs of the organisation. All potential risk areas may in fact be under adequate control. But, unless a periodic risk assessment is performed within a well-defined investigation and reporting structure, the computer services manager has no rational framework on which to base his claim of adequacy.

DEVELOP GENERAL MANAGEMENT SKILLS

In chapter 2 we set out the skills required by the successful computer services manager and emphasised that they are general management skills rather than technical skills. The responsibility for obtaining these skills falls primarily on the computer services manager himself. Candidates for computer services management positions therefore need a higher standard of business management education than their predecessors required. Those who have been in such positions for some time may need to convince senior management that it is in the interest of the business for them to receive additional management training.

BEWARE OF COMPLACENCY

Today's computer services manager is being presented with many challenging and exciting opportunities and this situation is likely to continue into the foreseeable future. But those opportunities can also bring threats — threats to his very existence if he does not respond to the challenges presented. If he is to survive in his position, the computer services manager must make every attempt to anticipate where and in what form the challenges will arise.

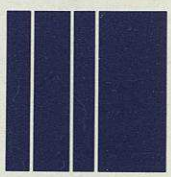
Our final guideline is therefore to warn computer services managers that they cannot afford to be complacent. They operate in an ever-changing environment. To succeed in their primary role of providing an adequate level of service to their users, they must be continually re-examining all aspects of their function. Users' needs and perceptions of an acceptable service will continue to change. A service that is adequate today will be unacceptable in the not too distant future.

CONCLUSION

The purpose of this report has been to provide guidance to computer services managers as they face up to the opportunities and threats presented by the changing computer services environment. To counter the threats and to take advantage of the opportunities, computer services managers must recognise and come to terms with the changes in the information systems discipline that will affect their particular environment. We have identified those changes as being technological, leading in turn to changes in user attitudes, which in turn lead to changing responsibilities for the computer services department.

The changes will also fundamentally affect the staffing profile of the computer services department. There will be less need for traditional computer operators, but more need for a smaller number of highly qualified specialist staff. Managing the changes implied by this shift is perhaps the greatest challenge facing computer services managers today.

The report has shown that computer services managers need to prepare themselves and their organisations to cope with the impending changes. In order to provide an effective service of unassailable integrity they must acquire the general management and interpersonal communication skills which they need to direct and control the function in a way that will achieve its full potential.



Butler Cox & Partners Limited
Morley House, 26-30 Holborn Viaduct, London EC1A 2BP
☎ 01-583 9381, Telex 8813717 LNCO

Belgium & The Netherlands
SA Butler Cox NV
Avenue Louise–479–Louizalaan,
Bte–47–Bus,
Bruxelles 1050 Brussel
☎ (02) 647 15 53, Telex 61963 BUTCOX

France
Butler Cox SARL
Tour Akzo, 164 Rue Ambroise Croizat,
93204 St Denis-Cedex 1, France
☎ (1) 820.61.64, Telex 610789 ASFRA

United States of America
Butler Cox & Partners Limited
P.O. Box 590, Morristown, New Jersey 07960, USA
☎ (201) 285 1500

Switzerland and Germany
Butler Cox & Partners Limited
Morley House, 26-30 Holborn Viaduct, London EC1A 2BP
☎ (London) 583 9381

Italy
Sisdoconsult
20123 Milano–Via Caradosso 7–Italy
☎ 86.53.55 / 87.62.27, Telex 311250 PPF MI

The Nordic Region
Statskonsult
PO Box 4040, S-171 04 Solna, Sweden,
☎ 08-730 03 00, Telex 127 54 SINTAB