1984

Senior Executive Perspectives on Effective Management of Information Technology

Robert K. Mautz
The University of Michigan

Alan G. Merten
The University of Michigan

Dennis G. Severance
The University of Michigan

Follow this and additional works at: http://aisel.aisnet.org/icis1984

Senior Executive Perspectives on Effective Management of Information Technology

Robert K. Mautz, Alan G. Merten and Dennis G. Severance
Graduate School of Business Administration
The University of Michigan

Introduction

Which of your company's activities cause you the greatest concern from an internal control point of view? What is the extent of your company's dependency on the computer? If a newly appointed chief executive officer asked you for advice on how to improve the effectiveness of his company's use of information technology, what advice would you give him?

These and many other questions were addressed to senior managers of U.S. corporations over the past four years in a series of studies directed at defining executive concerns and management controls (Mautz, 1980; Mautz, Merten and Severance, 1983; Mautz and Winjum, 1981).

The first study by Mautz et al., (1980), was directed to determining the internal controls in major corporations. In response to a series of questions to identify the major concerns of senior executives, "computer systems" was cited by more than 60% of the respondents—more frequently than any other item. Data for the assessment were drawn from both a widely distributed questionnaire and from personal interviews with more than 350 corporate executives. The questionnaire was distributed to the chief financial officer in 2,000 corporations and was completed by 673 of these firms. The interviews were conducted in fifty corporations with the chief financial officer, controller, legal counsel, internal auditor, senior information systems officer, and various staff and operating executives. These interviews revealed that executive concerns with computers include both the potential for disaster and the possibility of competitive disadvantage (See Table 1)

How should senior and functional executives deal with this state of affairs? On the one hand, they are forced by competitive pressures to apply the productivity leverage offered by computers; on the other hand, they are warned of the serious potential for computer misuse and abuse. A follow-up study was recently completed in an attempt to provide an answer to this question (Mautz, Merten, and Severance, 1983).

The next section will report on the nature of the problem as seen by senior managers and the solutions proposed by selected companies.

The Problem

Corporate executives were aware of their organizations' increasing dependency to computers, both for operational control and for information purposes. In addition, computer-related expenditures claimed as much as three percent of total sales, were sometimes measured in hundreds of millions of dollars, and were typically growing at fifteen to thirty percent per year. Information systems or data processing departments were noted for high personnel turnover, budget overruns, late projects, multi-year backlogs, absence of long range plans, and a general dissatisfaction by line managers with the quality of the service that they were provided. When these facts are coupled with the widespread belief that computer specialists feel more allegiance to their technology than to the company that employs them, then the basis for management's uneasiness is clear.

More specific insights into the nature of the disaster-related risks faced by corporations were obtained during interviews with the chief internal auditors. They were concerned with both computer failure and computer abuse. Many companies have come to rely so heavily on their computers for the daily processing of transactions and control of operations that a serious computer breakdown could lead to a substantial curtailment or stoppage of operations. Few of the companies studied were adequately prepared to cope with such a system failure.

Computer abuse was the second concern of the auditors. Sensitive corporate data, especially financial and accounting data, are stored in computer memories increasingly accessible from remote terminals. Such data, are thus exposed to potential manipulation, misuse, or destruction through operations that require only a fraction of a second for completion, and which can be initiated through terminals hundreds of miles away. Companies that are extremely cautious about cash control may quite unconsciously permit other employees to "get their hand in the till" through the initiation of transactions at data processing terminals.

Technological developments like mini and micro computers and distributed database systems increase the availability of computers and computer terminals. Auditors suggest that predicted advances in office automation, user-friendly languages, and telecommuni-

Table 1

Senior Management Concerns

POTENTIAL DISASTERS

1. Complete or partial interruption of business activities.

2. The destruction of accounting and control records.

3. Material inaccuracies in accounting and control records.

4. The manipulation of accounting and control records to cover or effect irregularities.

5. The exposure of sensitive corporate information.

COMPETITIVE DISADVANTAGE

1. The erosion of competitive position due to obsolete computer systems.

2. The inefficient use of scarce information systems resources (people, equipment, facilities, etc.).

3. Excessive information systems expenditures.

4. Information systems departments that are unresponsive to line management needs.

5. The dissipation of management energy in preoccupation with inappropriate or ineffective computer systems.

---

cations will increase the internal control risks still further. They fear that the ability to conceive and build useful computer systems may far exceed the ability to guard against possible misuses and potential attacks against these systems and the corporate assets that they control. They observe that many of the controls incorporated in financial systems today were devised only after a significant loss painfully demonstrated the need. Auditors frankly admit that the time and effort needed to certify the adequacy of controls even on existing computer-based system is far beyond their ability, given current expertise and manpower. They fear that current attempts to relieve the backlog for new systems by encouraging end user computing will lead to a flood of ill conceived, poorly documented, and under controlled systems.

Interviews with heads of information systems departments provided support for the auditors' fears. Within most companies, the information systems organization is viewed primarily as a service function—it collects, transmits, stores, retrieves, and displays information required by other departments of the business. Those who call on this department for service are principally concerned with the immediate availability of desired information. They seek quick, inexpensive, efficient and easy-to-use systems. The poor esteem in which some data processing groups are held today results precisely from their inability to meet this expectation of prompt service, economy, and simplicity.

Strong control is the antithesis of fast, inexpensive access to information. The analysis, design, and testing of a well-controlled system requires more time, and calls for more professional staff than a loosely-controlled system. The controlled system is generally less convenient to use, and is always more expensive to operate. Information system professionals tend to feel that their role is to provide ease and speed of computer access at minimum cost. Seldom are they motivated by, or trained in the need for controls.

The Executive Advice

The top management of many companies have successfully managed both the opportunities and risks provided by information technology. The systems installed in

these companies have resulted from a mixture of entrepreneurial spirit and technical competence plus appropriate amounts of policies, procedures, and organizational structure. A detailed study was made of a selected group of companies to determine what is installed and working, not in terms of computer systems, but in terms of management practices.

Twelve companies from the Fortune 100 which were reputed to have the problem of computer control well in hand were selected. We solicited advice from the chief executive officer, the corporate information officer, the executive to whom he reported, and the director of internal audit. In addition, senior executives from two public accounting firms and two major computer vendors were interviewed and their advice was incorporated. The spirit of the advice we sought is best captured by one of the favorite questions in our interviews: "Assume that your son or daughter has just been appointed chief executive officer of the Fortune 1,000th company, and comes to you for advice, saying: 'What do I do about my problems with computers?' How would you answer?" While the executives' responses were varied, the underlying advice was surprisingly simple: "Handle it like any other management problem!"

The prescription given by the interviewees typically included the following steps. First, be sure that the problem warrants your attention. Affirmative answers to the questions in Appendix 1 suggest that it does not. If it does, however, then take the time to become acquainted with the problem, its scope, and its nature. This includes participation in relevant short courses, use of consultants, and fact gathering through formal and informal discussions with managers involved with or affected by information systems.

The interviewees provided numerous suggestions as to how senior executives could determine the state of affairs within their organizations and in what areas information and action were probably necessary. Their advice led to the development of three sets of questions: one directed to the functional or line manager who has ultimate responsibility for effective utilization of corporate resources, one directed to the chief information officer or executives who supply services in the information technology area, and the last directed to the internal auditor who serves as a monitor and consultant on management and internal control in all areas for senior management.

Appendices 2, 3, and 4 are a composite of recommendations of our interviewees for questions designed to initiate relevant discussions within an organization. A senior manager might choose to put these question informally in a series of luncheon conversations or to submit them in writing and request written responses.

These questions are designed to lead to other questions, to initiate a dialog for exploration of opportunities, differences of understanding, reasons for complaints, and evidence of tasks performed well. Very likely these questions will initially draw out only symptoms of underlying problems such as "they are always late," "they don't understand what we need," or "our facilities are inadequate and we need more equipment."

In following up such responses, senior management should remember that its interest is in the underlying problems. "Why were they late? Did you change your specifications after they commenced their development?" "Were your people available to participate as promised? What did you do to get the project back on schedule?" Skillful questioning should get past the superficial symptoms quickly. What are the underlying problems? To get them all unearthed and identified may take more than one round of questioning and may lead to something akin to "shuttle diplomacy."

Keeping in mind a limited list of the basic management issues which are most likely to need attention within an organization will make the problem indentification process easier. Our executives suggested that the following ten issues are at the heart of most symptoms:

1. Inadequate provision is made, and insufficient resources provided for the investigation of competitive advantage through innovative applications of computer and allied technology. Functional managers are not encouraged to aggressively seek out areas where information technology can help. They fail to recognize the potential use in personal, local organization, or corporate activities.

2. The corporation does not have a clear statement of the mission and allocation of responsibility with respect to the specification, justification, design, development, testing, implementation, operations, maintenance, and auditing of computer-based information systems.

3. The information systems function is not located within the organization in a position that:

   a. Enhances the establishment of those priorities for service most conducive to attainment of company goals,

   b. Provides adequate access to senior management attention and to company resources, and

   c. Assures protection from undue domination by any one user.

4. The internal organization of the information systems function gives inadequate attention to the

operation of current systems, or to production of new systems which meet user needs, or to innovative applications necessary to maintain competitive advantages, or to the support of users who want to build their own systems.

5. Inadequate provision is made for controlling costs for both current operations and capital expenditures.

6. No effective provision is made for measuring the efficiency and effectiveness of activities that employ information technology.

7. Inadequate provisions have been made for the security of information systems facilities, hardware, software, and personnel.

8. Neither the internal audit department, nor any other quality control group provides expert and independent consultation to the information systems development activity regarding adequate control measures at the time systems requirements are first specified. There is inadequate follow-up to assure that such control measures are included before the system becomes operational.

9. Inadequate provision has been made for assimilating the information systems activity into the company in a way that assures information systems personnel attractive, long term career opportunities.

10. Senior management does not participate in monitoring the information systems activities with sufficient understanding to recognize existing or impending problems.

Corporate Action

A variety of strategies for dealing with each of these issues was suggested by our executives and are detailed by Mautz, Merten and Severance, (1983) and outlined here. Specification of the "best" solutions for each problem is tempting but must be resisted because both problems and solutions are so company-specific. The "right solution" to a problem in one company may not be the right solution to the same problem in another company. Differences in organizational structure, in available personnel, in the urgency of the problem, in competitive conditions, and in other factors all bear on the appropriateness of a solution.

At the heart of most management problems, however, are people problems. And these are often caused by a failure to define responsibilities in such a way that both the performer and those that interact with him understand what is expected. As outlined below, many of the actions suggested by the executives were designed to overcome these misunderstandings by assuring that the right people were correctly positioned in the right locations with sufficient resources and authority and a clear specification of their responsibilities.

Our interviewees suggested that one of the keys to successful utilization of information technology was the appropriate and clearly defined responsibilities of the line or functional manager, the chief information officer, and the internal auditor. As the capabilities and cost of technology has changed, these responsibilities have had to change. As responsibilities have changed, the characteristics and knowledge of the appropriate manager has also had to change. Where these changes have occurred, success has followed. Similarly, failure of the manager or his organization to make the necessary adjustements has led to inaction or disaster.

Collectively, our interviewees suggested sets of responsibilities. The line manager (see Appendix 5) is the ultimate deliverer of a corporate service or product. Information technology is only one of the areas in which he can spend the corporate resources allocated to him. He is responsible for selection of the areas of application, the expenditure of time and money on the project, and the system itself when it becomes a part of his operation. The level of his responsibility is the same whether he builds or buys the system himself or has it supplied by an internal information systems group.

The chief information systems officer's responsibilities are in the areas of system resources, service, and long-range planning (see Appendix 6). Like the line manager, the responsibilities of this position are changing dramatically. Our interviewees stressed the increasing importance of the managerial skills of the chief information officer. They also stressed the need for the CIO to become more a part of the management team, primarily with respect to how he deals with his peers in other functional or service areas and with his superiors. In no way has the current emphasis on user involvement in computer system development or user developed systems diminished the importance of the chief information officer in the minds of our interviewees. In fact, the opposite is true. As the technologies and their areas of application proliferate, the resource management, service, and planning functions of the CIO become more crucial to successful corporate use of the technology.

As information technology becomes more a part of the operations of an organization, the importantance of properly controlled use of this technology grows. System failure and abuse are no longer just slight inconveniences in the on-going operations of an organization; they can lead to large financial losses and bad publicity. Most of

our interviewees stressed that the responsibility for insuring that the control mechanisms was that of the line manager, and the responsibilities for properly installing these controls was that of the information system supplier. The internal auditor (see Appendix 7) plays a role of control consultant, critic, and monitor.

The roles and responsibilities of the three positions described above are meaningful only to the degree that they are well defined and clearly understood and accepted within the organization. Our interviewees stressed that direct top management involvement is essential for something positive to happen. If these new responsibilities are not viewed as important by executive management, and monitored in some way, then nothing will change. "If it doesn't get measured," we were told, "then it won't get done."

As was mentioned earlier, the underlying advice from our executive is to "treat it like any other management problem." Like any other management problem, it takes time, a certain amount of specialized knowledge, some formalization, and a measure of encouragement for productive results to appear.

REFERENCES

Mautz, R.K. et al. *Internal Control in U.S. Corporations: The State of the Art,* Financial Executives Research Foundation, Morristown, New Jersey, 1980.

Mautz, R.K. and Winjum, J. *Criteria for Management Control Systems* Financial Executives Research Foundation, Morristown, New Jersey, 1981.

Mautz, R.K., Merten, A.G., and Severance, D.G. *Senior Management Control of Computer-Based Information Systems* Financial Executives Research Foundation, Morristown, New Jersey, 1983.

Appendix 1

Questions for Senior Management

Do I have dependable evidence that our expenditures for information systems are both adequate and well spent?

Do I have dependable evidence that we are exploiting opportunities for advantageous use of the computer as effectively as any of our competitors?

Do I give as much time to information systems as I give to any other function of equal importance to the company?

Am I as familiar with the strategic plans for information systems as I am with similar plans for any other function of equal importance to the company?

Do I receive reliable, periodic reports telling me in understandable language how well our information systems are meeting their goals?

If I desire an independent, trustworthy, understandable evaluation of our information systems, do I know the persons who can give it to me?

Appendix 2

Questions for User Management

Those who are responsible for the effective use of information technology and who use the services of the information systems department, including line managers and such general officers of the company as the personnel officer, sales manager, and the controller. Not all of these questions are appropriate for all of these executives although each question should certainly be addressed to at least one of them.

Are you receiving all the information that you think you need from our information systems on a timely, reliable basis?

Do you know of any computer-provided information or other service utilized by others in our industry that we do not now have?

Do you think that what we do get from our information systems department is produced at reasonable cost?

What would you like from our information systems that you are not now getting?

What are you now getting that you do not want?

What requests have you made to our information systems people that have been rejected or delayed unreasonably?

What provisions now in effect are intended to keep information systems personnel informed on prospective changes in your activities or needs that might influence their work?

What was the most significant impropriety regarding computers that came to your attention in the last year or so? Why do you think it happened?

What do you feel is the likelihood of lost transactions, incorrect processing, and inaccurate information being generated by computer applications upon which you depend? How would you detect such occurrences? How do you prevent them?

How would loss of the computer for several days affect your operations? What would you do if this occurred?

Do you think you and the manager of the information systems department have similar views of your respective responsibilities in developing the information systems you need?

What additional skills or knowledge do you feel would most improve the information systems manager's ability to contribute effectively either to your needs or to corporate goals?

What do you feel would be an equitable procedure for allocation of information systems costs to using departments?

What could be done to enhance your control over the quality and cost of systems and services provided to you?

Appendix 3

Questions for the Chief Information Officer

A key person in control of information systems is the person to whom senior management looks for direct control, not only for the operation of the computer room and the production of regular reports, but who also accepts responsibility for the development of new systems and is the interface between the professionals in information systems and the rest of the company. This is the person to whom the following questions should be addressed.

Does the information systems function have a statement of its mission?

Is that statement considered appropriate? Reasonable?

In what ways would you change it?

Do the budget and resources allocated to information systems support that statement of mission? Are specific allocations made to long-range planning and research and development activities?

On what basis do you feel your performance is evaluated? Is this reasonable? Is it supportive of your mission statement?

Do the line and staff managers who come to you for service understand your mission and responsibilities in the same way that you do?

Do you feel that they and you speak the same language? Can you communicate with them effectively?

What are you doing to become better acquainted with their problems and business needs?

What do you think they should be doing to become better acquainted with your problems and operating constraints?

Ideally, where do you think information systems should be located within this company?

Are you satisfied with its present location?

Do you get adequate responses to your questions and requests for help?

Are you privy to the long range plans of the company?

What are the most serious personnel problems you face in your department?

How do you approach the problem of acquiring competent staff? In what ways do you direct their actions, monitor their progress, and measure their success?

How do you maintain the competency of your staff?

Who on your staff could replace you in an emergency? How have you prepared that person for such a contingency?

What are your personal career goals?

Do you think you can attain them with this company?

56

What personnel or organizational constraints do you feel most hamper your possible success? How might these be relieved?

Ideally, how should the information systems function be organized internally?

Does the present organization work reasonably well?

How would you change it?

Do you regard internal auditing as a help in the development of new systems or as a problem?

Do you or your staff members have difficulty in communicating with internal auditing?

What are you doing to help your staff members obtain a better understanding of the internal audit function in this company?

Appendix 4

Questions for the Director of Internal Auditing

Our earlier research suggested that in some companies the ability of the internal audit department to keep abreast of the technical progress in information systems was insufficient to assure that adequate control measures were included in new systems or that all processing performed by existing systems complied with stated control policies. Although the director of internal auditing does not have the same relationship to information systems that users do, that relationship may be crucial if senior management relies on internal auditing for monitoring the company's internal controls.

Does the internal audit function have a statement of its mission?

Are you satisfied with that statement?

How would you change it?

Does it give internal audit any responsibility for assuring that adequate control measures are included in new information systems? Do you think it should?

Do you believe that both the information systems manager and line management understand the scope of your responsibility as well as their own? Why do you believe this is so?

How much participation could you have in the development of new systems without interfering with the independence of your audit role?

What responsibility do you have for auditing the effectiveness and integrity of existing systems? Are you satisfied with that responsibility?

What responsibility do you have for evaluating the quality of the information systems function? Are you satisfied with that responsibility?

How competent in the technicalities of information systems are your staff members? Is this adequate? What measures are you taking to maintain or improve their competency?

Do you have "EDP auditors" on your staff?

Are they sufficient in number?

What is their computer training, their audit training?

How is their competence maintained? How are they motivated?

Appendix 5

Line Management Responsibilities

1. Remain informed on the potential impact of technology upon the operations, products, and services of their function.

2. Within the framework of corporate policies, identify specific application areas for information technology. Determine the appropriate source of the new technology, be it from the functional area itself, from corporate or local information systems groups, or from outside the corporation.

3. Develop specifications and justifications for needed information systems.

4. Analyze risk to assets affected by information systems and define appropriate control requirements.

5. Plan and define testing and conversion procedures for new systems before they are implemented.

6. Encourage compliance with all system control procedures.

7. Establish contingency plans for loss of computerized systems.

8. Classify all data transmitted to information systems or received therefrom according to its degree of confidentiality.

9. Assure that all data are provided with appropriate security at all times.

10. Formally evaluate the quality of the corporation's information systems services.

Appendix 6

Chief Information Officer's Responsibilities

To manage the organization's information systems resources efficiently and economically, the CIO must:

1. Develop, maintain, and monitor policies, plans, and schedules which direct the day to day operations of the information systems function.

2. Manage the information systems staff by establishing policies and procedures to plan, acquire, motivate, educate, counsel, evaluate, and promote quality personnel.

3. Establish policies and procedures to plan for, acquire, maintain, and replace computer facilities, including hardware, software, data communication, office automation, computer-assisted design, computer-assisted manufacturing, and such other computer-related resources as may be available to and effective for the specific company.

4. Develop and advocate annual budget requests which support the corporation's long-range information system plans.

5. Be accountable for information systems resources and costs.

The corporate information officer should provide line managers with timely, reliable, cost efficient, and easily obtained information systems services. To do so the CIO should:

1. Assure accurate analysis and specification of line management's information systems requirements.

2. Assure timely and reliable development or outside acquisition of systems which satisfy line management's specifications.

3. Provide technical support and advice to line management in the testing and installing of new information systems.

4. Assure efficient and reliable operations as well as timely modification of installed systems.

To assist in establishing long-term priorities for the corporation's information systems, the CIO should facilitate the definition of information needs both in the present and in the future. To do so he must:

1. Foster management understanding of the capabilities and the limitations of information systems technology.

2. Provide information systems counsel and education to management and others.

3. Track technological developments which may impact the corporation and disseminate this information to those managers who may find it effective in meeting their responsibilities.

4. Interpret information system implications of the long-range business plans of the corporation.

5. Assist management in developing long-range information system plans which support the stated mission and strategic objectives of the corporation.

Appendix 7

Internal Audit Responsibilities

1. Provide consulting advice to line management and information system staff on the design of controls for new systems.

2. Evaluate existing information system control policies and procedures on a regular basis to assess their need, adequacy and effectiveness, and to make recommendations for their improvement.

3. Monitor compliance with control policies and procedures once established by management.

4. Cooperate with the independent accountants in the performance of annual audits in order to avoid duplicate tests and excessive costs.

5. Provide senior management with assurance that the corporation's control systems are adequate.