regulated or quasi-private and public sector. This serves as an excellent grouping; I am sure that a good deal of preplanning went into the organization and invitation of the conference participants. Each section was written by the actual attendee, and the differences in writing style do not get in the way of the reader.

Although I am disappointed not to see any organization representing the financial sector (such as banking, insurance or brokerage) or heavy manufacturing, the range of organizations included is impressive and interesting. I would (with the enormous benefit of hindsight) have liked to see the private sector broken up into service and manufacturing groups, but one cannot fault the inclusion of any organization presented, with the possible exception fo having two international petroleum companies (Mobil Oil and Standard Oil of Indiana). The contributors also include Ciba-Geigy, TRW, Hughes Aircraft, IBM and Xerox.

The quasi-private sector includes two public utilities (Consumers Power and Pacific Gas and Electric), TWA and the Permanent Medical Group and Kaiser Foundation Research Institute. While I think the inclusion of TWA and Kaiser in this sector is a bit tenuous, this is a mere quibble.

The public sector includes the Board of Governors of the Federal Reserve System, the U.S. Army Material Command, the Los Angeles City Unified School District, the State of California and the University of California.

The book concludes with an appendix containing actual planning material from IBM, Mobil, U.S. Army Material Command and Xerox, as well as the actual survey questionnaire forms used to collect the information presented in the profile section of the introduction; a follow-up questionnaire on planning for information systems, and brief biographies of the individual contributors.

Almost anyone will be able to find an analogous organizational write-up with sufficient similarities to form a comparison with his or her own organization. To some, this will prove disheartening for they will see themselves far behind the leading edge. Yet, in other cases, the level of planning displayed is ludicrous, since it centers not on planning but on monitoring and control, and at the budgetary level at that. I have always found this type of reading most interesting, for it offers some insight into the inner workings of organizations which one would never have unless direct personal association were possible (like the "company confidential" stamp on the bottom of the reproduced IBM documents).

To some, the aspects of long-range planning are timeless, but it should be noted that the actual conference was held in April 1974 and thus the prepared material stems from 1973. The editors' foreword is dated July 1976, more than two years after the conference was held. The material, in terms of the evolutionary state of the specific organizations is thus seriously out of date. While I am somewhat aware of the publishing cycle, the extensiveness of this time lag is extreme and to some will seriously qualify the value of the book. The efforts being made by NSF and others to shorten materially the publishing cycle via automated text editing techniques will be much welcomed.

A last and final touch that is nice is the title and address of each of the participants, but due to job mobility and the over-three-year lag, this may also be seriously out of date.

All in all, *Strategic Planning for MIS* is a worthwhile book for actual corporate planners and in the MBA curriculum. The volume is not without flaws, but on balance it makes a positive contribution.

—Gene Altshuler

MISCELLANY

Compiled by James S. Ketchel

The Small Business Information Systems session at the 1977 NCC held at Dallas in June was organized as a combination paper, panel and audience-panel dialog, which was the result of only one paper in the small business area being accepted for presentation. Yet the audience attending the session was one of the largest at the conference, indicating a keen interest in the problems faced by the small business as it automates its information flows.

Frederick Francis Newpeck chaired the session and also presented the paper which set the scene for the discussion that followed. The full text of the paper appears in the Proceedings and the session was also reported in the June 20, 1977, issue of *Computerworld.* The paper covered a broad base, including why one should consider automation of information flows, the costs of automation, some reasons computer systems fail and a six-point plan to assure successful computer system implementation.

In the panel discussion that followed, J. Daniel Couger emphasized the importance to the firm of automating its lifestream systems first. He also stated that he thought the role of the consultant to a small business was that of an adviser. He said, "Insiders understand the firm and its needs better than the consultant, and through the data gathering and organization process, company personnel better comprehend the information flow and process for the firm. Not only is this a necessary step in proper specification development, it is essential to proper implementation and computer use. The job of the consultant should be to get the process started and to aid in the organization of the data."

William W. Cotterman agreed that a process of computer acculturation was necessary for successful MIS implementation, similar, he thought, to that required prior to successful computer use in Middle Eastern and Third World nations. Finally, Ted Cary, author of "Custom Programming in the Small Business Environment," *Computer,* September 1976, pp. 16–22, advocated the use of custom programming to tailor the software to the "personality" of the small business. The session ended with a half-hour discussion which clarified many of the points expressed in the session.

• • •

At the Computer Security Risk Assessment session at the 1977 NCC, two formal papers were presented: "Security Risk Assessment in Electronic Data Processing Systems" by Robert H. Courtney of IBM and "Problem Areas in Computer Security Assessment" by Steve Glaseman of the Rand Corporation (coauthored with R. Stockton Gaines of Rand and Rein Turn of TRW Systems Group). Two panelists presented their views on risk assessment and commented on the papers: Thomas Q. Stevenson of the U.S. Department of Agriculture and Brian Ruder of Stanford Research Institute.

The purpose of computer security risk assessment is to provide the management and users information on the losses that could result if computer security safeguards failed or were not implemented, the likelihood of loss-causing events and the amount of resources that would be reasonable to allocate for providing protection.

Courtney's paper presented a risk assessment methodology that has found considerable acceptance in the business community, although there are still many skeptics. He defines risk as the product of an estimate of the value of a particular data file (in dollars) and the expected frequency of losing that file (such as once every X years). The result, also expressed in dollars, is the exposure (relative to this particular file) of the organization per year.

Courtney illustrated this, as follows. Assume that a corporation stands to lose $150 million from a catastrophic event involving its computerized information system and all data files. Further, assume that such an event is expected with a frequency of .003 per year. Then the exposure of the corporation is $450,000 a year. The options open to the management are to tolerate the risk or implement additional security safeguards that will cost less than $450K per year and significantly reduce the exposure.

Both the assignment of dollar value to data files and the estimation of the frequency of losses are very imprecise activities. Courtney suggests that their measurement on the basis of orders-of-magnitude is adequate, and that more precision is not only impractical, but may be outright undesirable—as this may convey an impression that the methodology is more scientific than it really is.

Glaseman's presentation analyzed and critiqued the existing risk assessment methods (such as the one proposed by Courtney). He suggested that there is a need to understand better the risk assessment process, the motivations of potential intruders and the amounts of resources they need to exploit various vulnerabilities in computer systems. He called for more research in determining and assigning values to protected assets (possibly using nonmonetary measures), understanding vulnerabilities of computer system elements and determining the probabilities of their exploitation by intruders.

Panelist Stevenson presented a series of slides describing the structure of the risk assessment process as followed at the Department of Agriculture: obtain firm management commitment, set up a risk analysis team, define the need for security, evaluate existing security, develop a set of alternatives for improving security (if needed) and report to the management. Risk assessment, essentially following the technique by Courtney, takes part in the step dealing with definition of security needs. Stevenson suggested that an "embarrassment factor" could be a nonmonetary measure of risk that may get management attention.

Panelist Ruder has performed risk analyses for SRI customers. He pointed out that the development of a risk management plan and performing the risk assessment are difficult and costly when they are attempted for the first time by an organization. But even if the results will be rather soft, the organization has benefitted greatly from having established an EDP security program and learned a lot about its EDP operations, he said.

In the subsequent discussion with the audience it was brought out by the attendees that the risk analysis team itself may pose new risks; it would be one group in the organization that knows about all the vulnerabilities in the organization's computer systems and activities. Therefore, the team should not be excessively large, and its members be allowed to participate only on a need-to-know basis.

Courtney used the occasion to emphasize again that the main threats come from incompetent computer facility employees, not from sophisticated intruders from outside. Other threats after incompetents are dishonest employees of the organization and then various accidents such as fire or flood.

• • •

In the 1977 NCC session on Performance Measurement of the MIS Function, it was brought out that management has been slow in applying reporting and control techniques to EDP installations for basically two reasons:

1. Fear of impeding development of EDP applications.
2. Difficulty in collecting and allocating data processing costs.

Whether the costs of an EDP installation should be charged to its users, or considered part of the general overhead is a complex problem, it was acknowledged. However, the choice of method is less important to the control of the computer facilities than the way it is administered, the session concluded. Other opinions voiced are as follows:

A charging system should be implemented when demand for EDP services is such that the services become a limited resource and should be allocated among the users. A charging system should also be considered when management desires an accurate accounting for the cost of computer utilization. To answer the question of what to charge the users of an EDP facility, it is necessary to classify and accumulate the costs before allocating them. The costs should be classified as direct, indirect or associated costs. It is recommended that they be accumulated in the following cost accounting classifications:

1. Salaries and related expenses.
2. Occupancy and related expenses.
3. Equipment and related expenses.
4. Communication and related expenses.
5. Supplies.
6. Other operating expenses.
7. Allocated and unallocated expenses.

The functional cost center activities of the data processing facility must be identified for cost accumulation and work measurement. These activities vary with each individual organization, so each organization must define its own data processing activities. It is suggested that the hierarchy of the organizational structure be used as an initial classification of the functional activities for cost accumulation. In general, costs for most data processing installations can be accumulated into four major functional activities: administration, systems and programming development, technical support and data processing operations.

These are each composed of several subfunctions. For example, systems and programming development may be broken down into systems analysis, systems design, program design and so on. The degree of breakdown into subfunctions depends on how precise the allocation formula is expected to be.

If costs associated with each subfunction can be clearly identified, and work effort can be measured, rates can be established for charge-back purposes. If work effort cannot be measured, the function should be considered overhead and should be allocated accordingly.

Costs should be aggregated into functional cost centers for both management analysis and billing. The degree of aggregation is at the discretion of management because of the trade-off between specificity in analysis and increased data collection costs.

For each cost center, a measure of activity should be selected which will be a consistent indicator of the work achievable. This measure should be a simple, comprehensive and consistent measure of work performed. Procedures must be developed to measure the utilization of each function and to cost the use of each function. Predetermined rate or standard cost procedures are generally used to cost the use of functional work activity.

The allocation of costs to cost centers can be very subjective. Rules that are established for cost allocation should allow the accurate identification of true costs associated with a functional work activity. These rules of cost allocation will vary in each data processing installation according to the classification of costs among direct, indirect and overhead categories.

Computer resource utilization should be measured to provide a means of determining those resources which are application-program initiated plus operating system-initiated to be distributed to the users of data processing services. With the advent of multi-programming, successful utilization measurement depends on standard consumption rates based on expected utilization rather than on available time. Data must be collected relative to the CPU, internal storage, I/O channels and I/O devices to provide for accurate and consistent task accounting.

An automated cost allocation system which measures the utilization of computer resources should consist of a module to measure component utilization and a module to perform cost analysis and billing. The utilization measurement module collects data on the use of the major hardware components by both application and system program tasks. The cost analysis and billing module provides a recap of the accounting to allocate data processing costs among internal users. The measurement data elements may require two levels of translation into the actual bill, to be intelligible to the user and to provide information to the systems analyst on which components are the major contributors to the job cost.

The cost data for evaluating computer resource utilization can be used, not only for cost allocation to users, but also for the planning of new EDP installations, as well as for budgeting control over the operating costs of existing EDP facilities. The cost data should be incorporated as part of the information systems plan. The information systems plan should include:

1. A description of the information processing objectives.
2. A description of all planned application system development projects.
3. The organization and staffing of
   a) the applications system and programming department and a set of system development measurement criteria
   b) systems software department (technical support)
   c) operations department
   d) data control group
   e) data preparation group
4. An equipment and systems software configuration plan supported by expected work levels for each device and
   a) technical support measurement criteria
   b) operations performance measurement criteria
5. Communications network plan.
6. Management control plans, including samples of reports to be used by information systems management to control the activities.
7. Operating budget for each cost center.

• • •

In cooperation with ACM, the Department of Computer Science at Technion in Haifa has organized Israel's first conference on data bases, "Improving Usability and Responsiveness," to be held August 2-4, 1978, at Technion.

The program chairman is Ben Schneiderman, Department of Information Systems Management, University of Maryland, College Park, Maryland 20742. Four copies of papers ranging from 3,000 to 8,000 words, with illustrations counting 300 words each, should be sent to him by December 1. Sought are reserach-oriented papers, but not purely theoretical analyses or descriptions of specific commercial systems. Professor Schneiderman can be contacted by phone, 301-454-2548.

FROM OUR READERS

Incredible! The article, "MAPP: A DSS for Financial Planning," by McLean and Riesing in the Winter 1977 issue of DATA BASE, contains, in the fifth paragraph from the end, the most insensitive and offensive statement I have ever seen.

Perhaps one could somehow forgive the "proud fathers" of the original utterance, but it is more difficult to excuse the several sets of editors who let pass a sentence which is a deep insult to:

—Victims of Down's Syndrome and their parents.
—Those with a moral position against euthanasia.
—Persons from any Asian background.

JOSEPH L. OPRISCH
CONSULTANT, INFORMATION SYSTEMS
GENERAL ELECTRIC COMPANY
FAIRFIELD, CONNECTICUT

Editor's Note: The sentence in question, intended as an admonition to abandon badly flawed EDP design systems when remedies are too costly or time-consuming, was tasteless. It made reference to a form of congenital idiocy once commonly termed mongolism and advocated euthanasia for such a condition. The managing editor accepts full blame and apologizes, not only to the three categories of people cited by Mr. Oprisch, but to all DATA BASE *readers.*