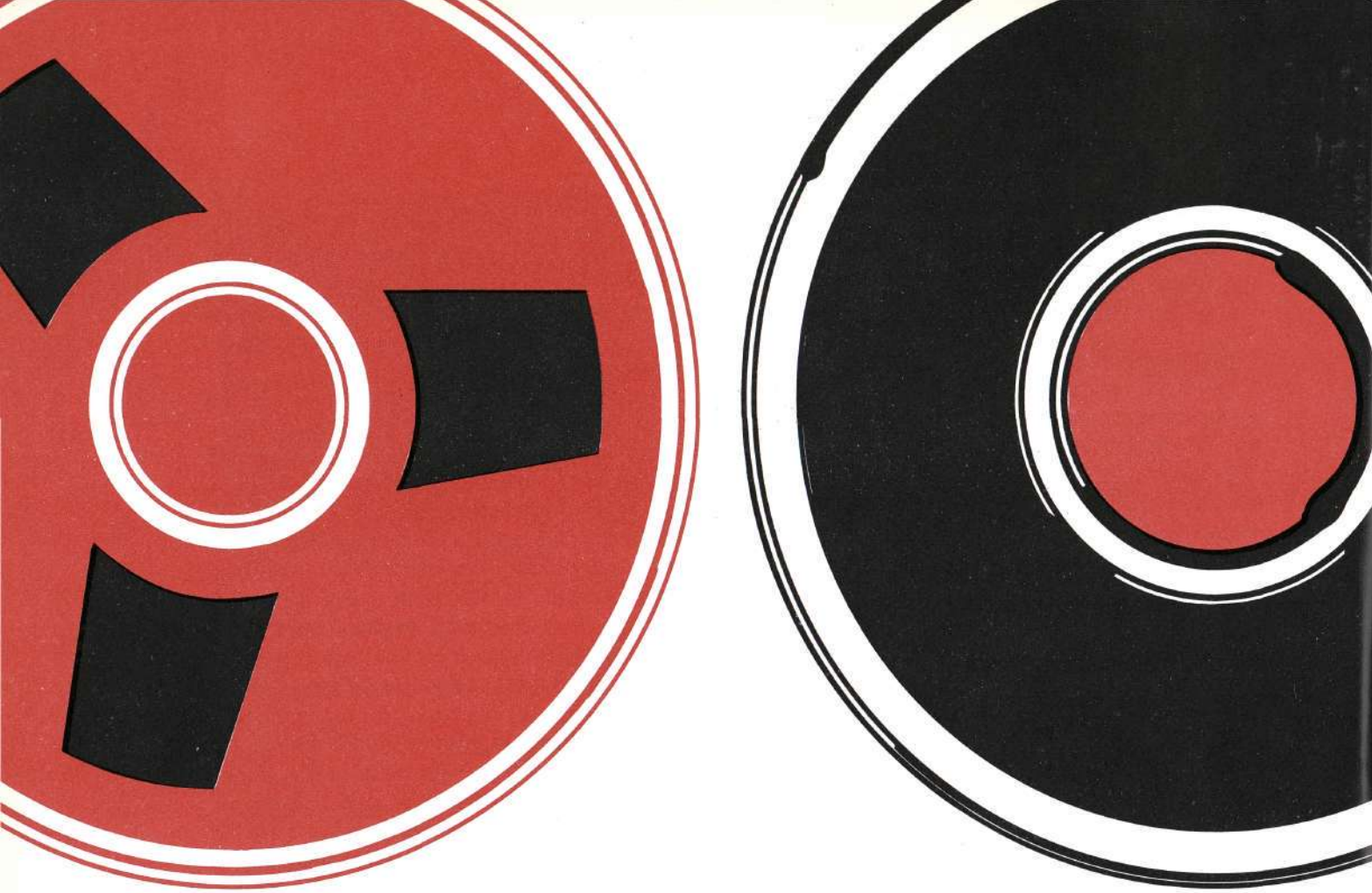
1968

How to protect your EDP records

Richard A. Levine



How to Protect your EDP Records

by Richard A. Levine

In today's complex world of computers, many companies are neglecting one of the basics of installation of computer systems—they often fail to safeguard the valuable records their systems produce.

Unfortunately, computer systems controls and operations procedures are usually considered last in the installation of the systems so that it is common for many manual systems to be automated with these important aspects still unsettled. It is especially unfortunate because it appears that the computer will assume an increasing role in company operations.

What may happen then is that most companies will increase their use of computers and have more data in machine-readable form but will be increasingly liable to the consequences of improper control and insufficient procedures.

Controls and procedures are vital because they provide respectively for detection of errors and inconsistencies and set systems standards, operator instructions and off-line protection for all relevant data.

The first aspect of EDP protection, systems controls, is divided into the two phases of editing—or analysis of information put into the records system

to insure correctness and completeness—and processing of records already in the system. Checking of fields to verify that data is complete and that quantitative data does not exceed set quantities, and checking of codes against predetermined values are types of editing.

As an example of the first type, the size field in input to a fashion merchandise control system should be checked for correct values. Incorrect values will affect the updating of the master inventory record in a later run. Input to an accounts receivable system should be checked to prevent unreasonable dollar purchase values from entering the system. This can be done by checking dollar values against a limit predetermined for each class of merchandise.

An example of the second type of editing is found in the use of codes to distinguish between debits and credits to input records, requiring that the correct codes be entered to allow proper processing in later routines. These codes should be checked in the edit routine.

Editing is accomplished usually by an edit routine used to create the input transaction file. When editing has been in programmed application, it often can be included by programming an additional routine. Thus the programs already debugged are not affected.

Processing of records already in the system requires the use of main processing and update programs. Therefore, if such controls are not considered in initial design stages, reprogramming will be necessary. The controls should include a sequence check of files, a check of computation results against predefined limits and an accumulation and verification of input and output record counts. In addition, hash totals—totals of account or item numbers for control purposes only—of numeric fields should be accumulated and checked against totals stored in trailer record.

To prevent destruction of live files, all output files should be label-checked to determine if the file name and reel sequence correspond with the program requirements. The retention cycle can be included as part of the label, and it too can be checked as part of the label verification.

The proper inclusion of these controls in system design and programming will be a valuable investment, helping to insure that correct EDP records are added to the company data files and existing records are protected from bad input data.

Proper operations, the second aspect of EDP protection, will insure efficient and reliable computer operation.

Although systems and programming standards have been widely discussed, it is important to remember that the main objective of systems and programming standards should be provision of a mechanism through which program documentation is written out and kept current in a standard manner. This will permit future maintenance of programs if the original programmer is not available—quite likely with today's heavy market demand for analysts and programmers.

These guidelines that apply to standards are applicable also to daily operating procedures. This is particularly important to companies that have union-organized computer personnel. Such companies should have a responsible management team prepared to continue the computer operations when necessary.

Likewise, provision should be made in advance for hardware failure, which is inevitable in the operation of any computer installation. The procedures to be followed when these failures occur will vary by type of equipment and its use in the installation. But the planning approach should include appraisal of each piece of equipment and the effects of its failure on the over-all processing system. There should be a determination of the consequences of each component's failure and a plan laid out for alternate methods of processing. For example, you might tolerate a printer failure for four hours, but you might have to use a comparable installation for off-line printing if the failure lasted longer.

These are several possible failure situations and their solutions:

Central Processor

1. *Revert to planned manual operation.*

a. Develop procedures to update files from time of failure with ensuing transactions;
b. Train people to run manual operation for critical output. For example, send orders directly to warehouse where computer is used for order processing system.

2. *Transfer to back-up facility.*

a. Determine that back-up facility has same configuration;
b. Determine effects on your company of use of a different shift;
c. Define logistical procedures for transfer of files and programs.

Peripheral Units

1. *Substitute output units.*

For example, a tape drive may be substituted for an on-line printer. However, efficient sub-

stitution requires that this alternative be documented as part of operations procedures.

2. *Transfer to back-up facility.*

3. *Switch to alternative peripheral unit of same type.*
For example, an application that requires three tape drives for running should probably have four as part of the configuration as protection against failure. A computer feasibility study should provide for protection against failure of critical units within the confines of financial reality.

4. *Operate in downgraded mode.*

The planning for protection against data destruction should include provision for protection of such vital data storage and report media as magnetic tape reels and disc files, program decks, flow charts, listings, program specifications, operating instructions, halt listings and control reports.

Protection of magnetic tape reels and disc files requires specific planning and written procedures. The procedures adopted to protect these files may be easily applied to the other media also. Records should be protected both on-line and off-line. On-line destruction can occur as a result of improper input, mechanical failure or program errors. The only protection against such destruction is the ability to re-create the master files from a stored back-up tape and a transaction history. This requires that the operations procedures be routinely followed and implies a "grandfather" system of cycling files through the system—retention of input transactions for three periods before destruction.

Off-line protection requires that the files be guarded from destruction by fire or other physical hazards. One preventive method is the use of non-combustible building materials in the computer room. This makes the files as safe as the equipment. However, the equipment can be replaced easily, but the same is not true for the files. Replacement of files would mean an expensive data conversion, even if the original source documents were not destroyed.

This form of protection may be modified by providing a fireproof safe in the computer room to prevent the files from exposure to high temperatures. This solution requires additional investment and constant enforcement to keep the doors of the safe closed, but keeps all files in a single, easily accessible place. While this latter method may be considered an advantage, it can also be a detriment if close control is not exercised to prohibit indiscriminate use of the files in debugging and testing in second and third shifts.

A third alternative is to retain back-up files in a distant location. The required files are then selected and transported between the computer room and remote location on a scheduled basis. This system requires the institution of the "grandfather" concept and thus solves the problem of re-creation because of on-line destruction. The benefits derived from this system are the reduced chance of destruction by careless programmers or operators and better protection from physical hazards. On the other hand, this system requires an increase in tape inventory and additional floor space.

Each of the alternatives has advantages as well as disadvantages. But the selection of an acceptable method must be based on factors peculiar to each company, such as frequency of updating, number of files, storage media, available floor space and available funds.