Southern Business Review

Volume 1 | Issue 1 Article 10

EDP Security- Necessity or Mania?

Victoria Wise
Georgia Southern College

COMMENTARY

EDP SECURITY—NECESSITY OR MANIA?

Victoria Wise

Businesses, large and small, are currently more vulnerable to losses through their electronic data processing activities than in the past. Reports of vandalism, fraud, theft, and even industrial espionage (e. g. a baking truck laden with antennas and cameras pulling up in front of the computer center and stealing computer-related information) are appearing in many of the business and administrative journals.

But how much of a threat to your organization are these activities? Most businesses appear to have one data processing objective in common—the accurate processing of the company's information, particularly for accounting purposes. These businesses have invested in and established many different controls and procedures for accuracy. Most businessmen do not seem to be concerned about the possible effects of embezzlement, fraud, forgery, theft, or destruction on the accuracy of the EDP function.

Perhaps the most prevalent reasoning behind this lack of interest in EDP crimes and disasters is confusion as a result of recent emphasis on security. There is no single answer to the security problem. Each organization has its own needs for EDP security even if all the data processing is done off the premises (e. g. by a service bureau).

With the increased government requirements for privacy of information in EDP systems, it is wise to take a moment to evaluate the effectiveness of the security of your organization's EDP procedures and the preventative countermeasures available to assist your organization in improving your EDP system.

There are three primary areas in which security considerations should be made. One area is the security of the physical equipment in the EDP center. A second item of concern is the security of the data in the EDP system. The third topic to consider is the security of the processing operation. In all of these areas the business EDP user is vulnerable to damaging effects either from erroneous information provided from bad data, or from nonproduction due to unauthorized manipulation, sabotage, other willful destruction, and acts of God.

At the same time the businessman must be on guard against overprotection and on the lookout for ways to cut the costs of security. Many items have appeared on the market, and the manufacturers claim these devices will provide "necessary" security and protection for any system.

In the remainder of this article, let us examine each of the three areas of EDP vulnerability and protection techniques available. Then one can determine which methods would financially and legally benefit his organization.

Physical Security

Techniques for the security of the physical EDP equipment can be divided into two categories—equipment protection, and personnel practices.

I. Equipment Security (the computer and peripheral equipment—hardware)

   A. Fireproof construction of the computer center.

   B. Early warning systems to detect fire, heat, smoke, and illegal intrusion.

   C. Appropriate security measures for providing adequate electrical power for communications supplements.

   D. The possibility of acquiring insurance coverage not only for the computer but also for business interruption due to damage to the computer.

   E. Refraining from placing the computer installation where it is easily accessible to persons entering the building.

   F. Appropriate safeguards for fire protection, humidity controls, and temperature controls.

   G. Formal or informal agreements with other companies with compatible equipment to use their facilities in an emergency.

   H. Alternative procedures for those systems upon which normal business operations are dependent.

   I. Alternative equipment and procedures for outside service bureaus with which you do business.

   J. Use of such equipment controls as: parity check, echo checking, dual gap heads (on magnetic tape devices), control lights and indicators, dual circuitry, file protection, storage protection, diagnostic routines, automatic retransmission, arithmetic overflow detection, and cryptographic devices (data scramblers, code schemes).

II. Personnel Practices (the people who work with or near the computer).

A. Closed circuit television surveillance plus electronic devices for detecting personnel entering data processing areas in possession of magnets. (The author is not recommending this technique, only stating its existence.)

B. Guards at the entrances of the computer center and identification badges worn by personnel having access to such areas.

C. More stringent checks on personnel before hiring, even night cleaning crews.

D. Limiting areas to which visitors have access.

E. Such policies as a code of ethics, nondisclosure agreements upon separation from the firm, the buddy system, job rotation, a training program, authorizations, and separation of duties.

F. A waste disposal procedure for printouts, carbon paper, and other media containing sensitive information. (One cannot emphasize enough the importance of this last technique. No matter what size the organization, computer printouts left in the trash cans or out in plain view contain job entry codes and other valuable organizational information.)

Data Security

There have been, and will continue to be, instances where computer personnel have intervened to manipulate files and programs. The techniques available to protect data include:

A. Employing the same physical safeguards that were mentioned perviously in dealing with equipment security.

B. Current backup sources of important files.

C. Non-accessibility to computer files by unauthorized persons.

D. A fireproof and lockable location used to store data files.

E. Control procedures whereby those files which are necessary for running a job are released only to authorized persons and are returned to storage immediately after their use.

F. File retention requirements and file reconstruction, if necessary.

G. Suitable facilities for the off-premises storage of key files and programs.

H. Standard procedures for program changes and alterations to be accomplished, including their authorization.

I. Tests for valid data in your programs, such as valid code check; valid character check; valid field size, sign, and composition; valid transaction; valid combination of fields; missing data; check digit; sequence test; and limit or reasonableness test.

J. Evaluation of security techniques for data stored on magnetic medium files (particularly tape).

   1. Administration of the library with all issues to and receipts from the computer operator being controlled by the librarian. (Many computer manufacturers offer tape and disk library control features.)
   2. Use of magnetically recorded tape labels.
   3. Use of "file protect rings" in the reels of tape that are not to be used for writing data during a run.
   4. Employing the "father-son" technique when updating or amending master files.

K. In the case of timesharing or assessing data via remote terminals, additional considerations for security include:

   1. Limiting the access to certain information to specific individuals, groups, or terminals.
   2. Investigating ways to control console intervention, such as data scrambling and locked recording devices.

(One way to control confidential data is to retain them on tape, disk, or other media in a safe until they are needed for processing. This method protects the coded data against fire, theft, or easy access for duplication to make a readable copy.)

Processing Security

Considerations for security as the data is processed can be divided into three control steps: input, processing, and output.

Input controls include using such techniques as a document register, batching, transmittal documents and route slips, cancellation and time stamps, matching, approvals, verification, self-checking numbers, hash totals, control totals, data checkers, and checklists.

Processing controls include crossfooting and negative balance tests; control totals; zero balancing; self-checking numbers; edit, reasonableness, existence sequence, completeness, combination, range, limit, data, and housekeeping checks; labels; passwords; and transaction logs.

Output controls to consider are: totals, checkpoints and restart procedures, setup procedures, sampling, reports control, console operating procedures, distribution instructions, exception processing, and computer audits.

Evaluation Considerations

These are the most prevalent security techniques. In looking at each item mentioned, one should remember that many of the techniques available cost more to implement than the value of the data being protected.

When one reads or hears some of the current computer "scare" stories, he should look for evidence to prove that they are really true. For example, several of the most popular fables involve the wiping out of complete tapes by magnets.

Research by data processing managers has indicated that approximately 12 centimeters between the recording medium and the magnet provide adequate protection against erasure. The 3-M Company advertisements claim that magnets do not completely erase tapes but that they can distort the accuracy of the information stored on the tapes.

Security is becoming more necessary as a result of current privacy legislation. At that same time, one should be on guard for little-truth "horror" stories and devices guaranteed to solve all security worries and problems. The manufacturer of the EDP equipment and the data processing personnel in the organization are the best sources of information for revising EDP security.

Ms. Wise is an Instructor in the Department of Management in the School of Business, Georgia Southern College.