File Control: The Heart Of Business Computer Management

by
William G. O'Brien
Assistant Professor
School of Hospitality Management
Florida International University

Even though computers are an everyday part of the hospitality industry, many managers lack the knowledge and experience to control and protect the files in these systems. The author offers guidelines which can minimize or prevent damage to the business as a whole.

The past three years have seen an explosive growth in the use of computer management systems in every part of the hospitality industry: from computer controlled electronic door locks to menu analysis. Some of the equipment being installed today did not even exist as little as a year ago, and systems have rapidly increased in capability and complexity. Equipment is installed today and becomes obsolete within the year. It is not surprising that too few hospitality industry managers have accumulated the experience required to exercise proper controls over computer management systems.

In some properties, the lack of control is visible on a casual walk-through. For example, an otherwise well-run restaurant has all its vital records, programs, and computers concentrated in a single room off the kitchen, or a fine hotel has placed its entire computer center in a showroom environment near the lobby. One franchisee hires a college student to program custom features into its back office accounting programs because the computer vendor wanted $2,000 for the change. In a large resort, a night auditor drops back-up tape cassettes into a drawer beside the central processing unit. In another resort, the newly-hired director of food and beverage complains of having to learn the computer system by asking questions of cashiers.

Each of these businesses has invited the financial equivalent of a heart attack. At other properties, it may take a few questions to bring out the problems: "Which files do you back up?" "Where do you keep them?" "Does your fire insurance cover the cost of reconstructing files?" "Who has access to the operating system?" "Do you have a training manual?"

Data Files Are Irreplaceable

In the examples mentioned above, experienced and knowledgeable managers exposed their properties to needless risk because they neglected a simple fact of business life: Of the three components that make up any business computer system (data files, programs, and hard-

FIU Hospitality Review, Volume 3, Number 2, 1985

ware), it is files that are most important, perhaps irreplaceable, to the business.

Recognition of this fact actually helped one property whose computer system was gutted by a small fire. No business information was lost because a back-up copy of each important file had been stored in another building. Insurance covered equipment, interim data processing, and a start-up of the replacement computer. An aggressive management actually used the occasion to upgrade to a newer computer from the same manufacturer. The business found itself in a better position after the fire.

In another case, a newly-hired manager was confronted with a wall of computer jargon from an uncooperative data processing division. She opened communication by asking for the name of each file maintained by the computer system. This led to a discussion of the type of information each file held and the kind of protection it needed. She was then able to set policies and assert her authority. In this case, the computer specialists had become so preoccupied with the technical aspects that they had forgotten the business aspects of the information they were processing.

To the computer programmer, all files are merely collections of data. Programs accept data, perform calculations on it, and store it in files without any regard to what the data means. To the business person and to the data processing specialist, however, the distinction between a file which is about business assets and a file which is itself an asset should be important.

There are two kinds of data files:

- **Files of extrinsic value.** An example of this kind might be a wine inventory. As sales are made and new shipments are received, the computer updates the file. This information might come directly from a point of sale terminal or might be entered manually by an employee. At the end of each accounting period, another program would print the file in the form of a check-off sheet. Someone would then perform a physical inventory and report any variance from what the computer program predicted. The final step would be to run a program which would correct the computer file to reflect actual inventory. Then the cycle would begin again.

This type of file merely tracks what is taking place in the business. If it contains incorrect information, or if it is destroyed, there may be some degree of inconvenience, but no guarantee of a loss. That is, changing the number of bottles in the file does not directly add to or detract from the assets held in the wine cellar. The information in such a file normally has no intrinsic value.

However, such a file can have substantial indirect effects on asset values such as causing management to over order perishables, with consequent spoilage, or to pay taxes on inventory that does not exist.

- **Files of intrinsic value.** In the second type of file, the information itself has value over and above its value as a business tool. Sometimes, the modification or destruction of such information can have

FIU Hospitality Review, Volume 3, Number 2, 1985

a direct, one-for-one, or even leveraged effect on asset values. Profit can be affected directly, indirectly, or in both ways. There are several ways in which the information in computer files can take on intrinsic value:

- The information is money in the legal sense. For instance, figures moved about in banking system computers do not represent dollars; they are dollars. If the record of a dollar amount is erased from all computer files, then that money ceases to exist.

- The information is money for all practical purposes. The accounts receivable file is an example of this type of file. For instance, a business might use this file to obtain a loan or actually sell the accounts for cash. A potential thief need only change the numbers stored in such files.

- The information is valuable and can be sold. An example might be a customer list which would have value to advertisers. Here a potential thief need only copy the file. It is not uncommon for dishonest employees to sell copies of such lists repeatedly.

Files Must Be Protected

File security requires a systematic approach. Start by finding out what files, by name, are used by the computer management system. Then determine what type of information is stored in each. Also, it is useful to know how big each file is. File size is measured by the number of alphabetic characters stored. Each stored character is called a byte. For instance, a file which contains 300,000 bytes (letters of the alphabet) would hold about 75 pages of printed text (assuming 80 letters per line and 50 lines per page).

Next, rate each file in terms of its value and the type of protection it needs. Files may need security against destruction, theft by unauthorized copy, or entry of false or erroneous data. The kind and degree of protection a file requires depends upon the type of information it contains. Put the most effort into protecting the most valuable and easily damaged assets.

Determine the following for each file: Who should have access and when? How often should it be backed up? Where should the original and back-up copies be stored? Which individuals will be responsible for making back-up copies? Consider how much each person should find out about what he or she needs to know about the system and how new employees will be trained. The objective should be written procedures for anticipated or possible events such as periodic file back-up, new hires, disasters, etc.

Then put the procedures in writing. Use simple, step-by-step language or people will ignore them. If necessary, rewrite vendor documentation to make it clear to employees. Take steps to ensure documentation does not vanish as employees leave.

FIU Hospitality Review, Volume 3, Number 2, 1985

Conduct drills periodically to see how well the procedures are working. For instance, it might be a good idea to turn off the computer power during a slack time. Perhaps a trusted employee can be assigned the job of "stealing" a file. Things may get a bit frantic around the front desk or in food service during the drill, but well-trained people will cope. They may even enjoy the change of pace.

Take corrective action when problems surface. In one restaurant, guest checks were being lost every time there was a momentary loss of electrical power because the manager was not following the procedure recommended by the vendor. This continued for months even though one phone call to the computer vendor would have corrected the situation.

Keep the procedures current and available to employees. If new employees seem overly confused by the computer system, the procedures probably need to be clarified. Do not depend upon old employees training new hires. Some information gets lost each time information is passed verbally.

Currently, business files are stored on disk or, to a lesser extent, on tape and tape cassettes. The disk allows information to be transferred at a higher rate than tape. Also, a disk system has the ability to move directly to any required information while a tape unit wastes considerable time reading through many feet of tape to reach the same data. For these reasons, disks have displaced tapes, except where it is desirable to store a large amount of seldom-used data at the minimum cost, such as file back-up.

Because the fixed hard disk holds far more information than the floppy disk, and because it is enormously faster, many property management systems and the larger food programs have been written for it. A typical storage requirement might be for 5 million characters of information (5 megabytes) immediately available. On an IBM PC/XT this would use most of the available disk space. The same files would require about 16 floppy disks. Clearly, the hard disk has operational advantages.

However, from the standpoint of a cautious manager, the hard disk alone is not entirely satisfactory. For one thing, it is an integral part of the computer system. A common disaster could destroy both. Recognizing this, one might then try to protect the entire system against all possible disasters. This scattershot approach guarantees that none of the measures taken will be truly effective.

Many Details Should Be Considered

One of the most important procedures will be file back-up. Copies of essential information should be in a separate location, preferably in a different building from the working file so that no natural or human disaster can destroy essential information.

How often files should be backed up — whether daily, weekly, or monthly — depends upon how essential the information is. Some organizations merely preserve older copies of files which are designated Grandfather, Father, and Son copies.

FIU Hospitality Review, Volume 3, Number 2, 1985

If equipment is not modern, it is unreasonable to expect frequent file back-up. For instance, some tape cassette back-up systems may require hours of continuous recording to back up a hard disk.

Although back-up copies are recorded on floppy disks or cassette tape, printed copies might be advisable if manual operations are to continue during periods when the computer system does not function.

Magnetic tapes and floppy disks are susceptible to electrical fields caused by equipment such as color T.V. sets and microwave ovens, as well as to heat, insects, dust, and the like. One restaurateur kept floppy disk back-up files in a cool, dry, insulated cabinet in his home. Unfortunately, he kept a magnetic flashlight in the same cabinet.

Sooner or later, every property will have its fire, flood, careless mistake, or disgruntled employee. When the target is the computer system, good file control can minimize or prevent damage to the business as a whole.

FIU Hospitality Review, Volume 3, Number 2, 1985