1970

Embezzlement through the computer

Kenneth C. Cole

Embezzlement Through the Computer

by KENNETH C. COLE
Partner, San Francisco Office

Presented at the Western Area Conference of the Financial Executives Institute, Seattle—June 1970

ONE OF THE MAJOR PROBLEMS of American industry today, embezzlement by employees, is believed to cost U.S. companies at least $3 billion a year. Theft by employees is estimated at another $1 billion. One source has estimated that about 30 per cent of smaller businesses fail because of employee dishonesty. From all indications, known employee crime among companies of all sizes is increasing at the rate of about 15 per cent a year.

HIGH-LEVEL PERSONNEL INVOLVED

One aspect of the trend is even more disturbing than its size—the identity of the people embezzling, stealing, selling corporate secrets, and taking bribes. According to some authorities, the bulk of the loss today is caused not by the rank and file, but by the managerial class. One study indicated that of discovered company frauds in excess of $60 million, 62 per cent were committed at the supervisory level or higher.

Investigators' files are filled with records of executive disloyalty and dishonesty. In one recent case, a $300 million-a-year eastern manufacturing company discovered that eleven department heads, each with at least twenty years of company service, had been taking kickbacks from subcontractors for the past five years. In another recent instance, the head of the computer department of a leading credit card company, resentful of top management, erased computer tape records storing hundreds of thousands of dollars' worth of accounts receivable.

COMPUTERS PRESENT NEW PROBLEMS

Many decades of auditing experience have provided a wealth of fraud cases involving manual accounting systems. Auditors use these case histories to familiarize themselves with the methods of defrauders. Changing technology has created new problems, and the electronic data

processing system necessarily forces changes in the methods used by defrauders. We cannot wait until a substantial history of actual cases of fraud committed in EDP systems has accumulated before studying the matter. Attention should be devoted as soon as possible to the problem of detecting the possibility of such frauds and of preventing them.

Effects of EDP Not Recognized

Suggestions of the possibility of fraud in EDP systems too often have been dismissed as being practically impossible for three reasons: (1) computers cannot be dishonest; (2) such a fraud would be too complex; or (3) internal control procedures prevent the same person from having access to valuable assets and to the records of those assets. Many corporate officers still do not acknowledge the need for additional internal controls in computer accounting systems. Recently a professor at the Harvard Business School observed a general condition of poor control and security in computer operations, even in companies that are well managed. This poor control situation can be attributed to a variety of reasons, including:

- The inbred experience of EDP personnel, who are primarily interested in making the machine run;
- The financial problems of making the proper investment in good documentation; and
- The lack of understanding on the part of non-EDP supervisors concerning what the data processing control needs are.

This lack of controls is odd in view of two conspicuous qualities of computers. On the one hand, computer technology, with its reliable detection and recording capabilities, frequently makes possible new and *superior control techniques*. But on the other hand, it appears to provide more powerful and sophisticated means of embezzling. Although the accounting profession recognized this paradox early and started to develop necessary fraud prevention and detection techniques, their efforts have been meeting resistance.

False Sense of Security

Apparently the need for well developed controls has not been acknowledged generally because executives have been lulled into a false sense of security. Many undoubtedly credit computer accounting systems

with a greater resistance to tampering than the facts justify. Others probably hesitate to require protective measures because of the sheer complexity of the technology.

Many executives in charge of highly intricate computer systems openly admit they haven't the foggiest notion of the nature of this tiger they hold by the tail. One administrative v.p. confided that, although he is in charge of the EDP Department, if he wants to know what's going on he has to ask one of the $150-a-week operators. He is praying that they are all honest or he could be in an enormous amount of trouble.

THE RECORD TO DATE

A leading computer expert at M.I.T. has said that if he were a crook, he would work today through computers.

An article in a recent *Wall Street Journal* quoted a prominent data processing specialist as saying that he could steal a company blind in three months and leave its books looking balanced. His method: electronic embezzlement; his accomplice: the company's own computer.

Increasingly, business transactions that formerly were recorded on ledger pages are being translated into magnetic impulses in a computer's memory section. It's a relatively simple matter for a swindler with technical know-how and a little imagination to program a computer to steal from a company. All too often corporate executives fail to question the reliability of financial results that emerge from complex, million-dollar machines. They simply forget that the machines have been built to do whatever the operators direct. There's nothing to stop them from working quite efficiently for the dishonest.

The head of a large U.S. corporation task force seeking to find methods of auditing computers used by his company has estimated that many companies already have been hit with heavy losses through computer embezzlement, but their managements don't know it. He predicts that within a few years someone will uncover a computerized embezzlement that will make even the most recently publicized swindles seem puny in comparison.

EMBEZZLEMENT CASES REPORTED

Employee criminality represents a genuine danger in the operation

of computer accounting systems. Over the past few years, the press has carried a number of reports of specific incidents of such conduct. These reports alone should have been sufficient to trigger your serious thinking.

State Agency

One day in August 1968 two New York City policemen's suspicions were aroused by the nervous manner of four men whose car they had stopped for a routine traffic violation. They opened the dash compartment and discovered an envelope with about 100 uncashed Neighborhood Youth Corps checks. Newspaper readers the next morning read the story of how six staff members had systematically milked the antipoverty project for nearly a quarter of a million dollars with the help of an unwitting accomplice, a computer.

Investigators found that a computer had been programmed to issue paychecks to hundreds of nonexistent youths, supposedly employed on an equally fictitious summer project. Had the scheme gone undetected until fall, said authorities, the coded cards representing the phantom work force could have been removed, conceivably leaving the computer with no memory of the embezzlement and the city without a clue as to how the funds had been taken or by whom.

Stockbrokerage

To date, one of the largest single losses that has been publicized was suffered through the corruption of a computer several years ago when one of the most reputable brokerage houses on Wall Street discovered that it had been defrauded of $250,000 by its trusted computer operations director.

The executive simply dropped by the office on Sundays and programmed the computers so that corporate funds were siphoned into two dummy accounts set up in his name and his wife's. The transfer was accomplished so smoothly that it appeared the monies had been used for stock purchases. He then made entries indicating sale of the stock supposedly bought and pocketed the cash.

Sensing something not quite right with the twin accounts, another officer of the firm, upon examining them, turned up the irregularities. Later, the firm's president stated that the computer executive's system was absolutely undetectable. They had no inkling that such a thing was

possible and, if the dishonest executive hadn't explained it all later, step by step, they probably would still be stumped.

Wall Street was still jittery over this computer scandal when a second case came to light, this time involving a data processing manager who over a four-year period had tapped the till for about $81,000 by instructing the computer to issue checks to fictitious payees, all checks being mailed to his home. His racket might be still flourishing had the Post Office not returned one of the phony checks as being "incorrectly addressed," which aroused the suspicions of a clerk.

A company spokesman said that they would be foolish to explain the details of his scheme unless they wanted someone else to attempt the same thing.

Banking

Computerized check handling by major banks makes them highly vulnerable to these crimes. One publicized swindle of this nature occurred in the Midwest, involving a part-time programmer with champagne tastes and a beer pocketbook.

The programmer had been assigned to service the computers of a large Minneapolis bank. He immediately opened a special checking account with the bank in question and inserted a change in the computer program that gave the mechanical brain a mental block when confronted by one of his checks. The computer would simply pass the checks for payment despite his insufficient balance.

This programmer's criminal career ended abruptly a short time later when the computer broke down, requiring several days of hand-processing the checks, one a blatant bouncer he had written. At the time of his arrest he had managed to bilk the bank of about $1,300.

Retailing

A bright young programmer, who decided he and his friends did not have to pay their bills for purchases from the store that employed him, simply inserted a routine in the billing program to transfer all charges in his own and his friends' accounts to a suspense account, which did not appear in detail but was included in the trial-balance total. This went on until the auditor, using the magnetic tape billing da-

ta under special routines for confirmation purposes, produced a run listing a substantial unexplained account.

Service Bureau

A recent $1 million embezzlement should stir some disquieting thoughts for companies that have their data processing done on outside computers.

A service bureau owner in Salinas, California, was sentenced in January 1969 for one to ten years' imprisonment for grand theft and forgery. For nearly six years he had embezzled money from clients. Only when a small-town bank became suspicious of the size of a check made out to a labor organization was he caught and brought to trial.

The defrauder had used his computer to budget embezzlements so easily that within a year he was able to steal $250,000 from a fruit and vegetable shipping firm. Apparently he had discovered that the firm had no complete audit trail. His next step was to make the company believe that the produce was costing more than it actually was, so that operational costs, profits, and other items stayed in balance. This he managed by keeping the balance carefully regulated through having the firm's accounting work done at the computer service bureau he had set up in the meantime. Here he budgeted just how much he should embezzle during a specified period by using both the false and the real data in different computer runs and by comparing the results.

REVEALED INCIDENTS LIKE AN ICEBERG

The low number of reported incidents is no indication of the true extent of the problem. Companies generally are reluctant to publicize incidents that are resolved short of formal legal action, and frequently even legal steps are hushed up. The reported experiences do indicate, however, that serious abuse is possible and that the problem deserves close attention at high executive levels. A long time ago, extensive internal control techniques had to be established for noncomputer accounting methods. Today the introduction of computers has not reduced vulnerability to normal dangers. Simple logic supports this fact: The factors that encourage criminality are present in both situations—people are involved and substantial ill-gotten gains are possible. In fact, the devices

provide new challenges to skilled persons who relish the opportunity to beat a system.

Even with the existence of elaborate internal control techniques, efforts have been made over the years to defraud companies that use non-computer accounting systems. It would be unthinkable for a company to have a traditional accounting system without a wide array of checks and controls to prevent and detect fraud and embezzlement by the persons engaged in its operation. Computer systems have many of the same vulnerabilities and some new ones as well. Hence, it is reasonable to conclude that computer accounting systems are not only vulnerable to efforts at fraud and embezzlement, but that they will become more so as operators and other personnel become more sophisticated about their workings.

COMPUTER FRAUDS BY EMPLOYEE POSITION

Any more detailed discussion of frauds in a computer system requires a consideration of exactly who could commit the fraud and how.

Machine Operator

Because of the apparent ease with which the machine operator can use console intervention, most discussions of fraud in EDP systems have been concerned with fraudulent action by him.

Normally the machine operator would have access to cash when checks are the input or output of the computer, such as in banking operations and disbursement routines. If the machine operator diverted a check, he could attempt to conceal the act by entering a false transaction via the console, or by inserting a transaction by forging a source document that would become the basis for input preparation, or by preparing the machine-readable input himself. Obviously, all of these frauds require a detailed knowledge of the computer program, and a programming fraud would require the ability to program. Thus, the greatest danger of fraud in a computer system exists where there is only one systems specialist who is at once the operator, programmer, and system designer. In smaller installations this would be the familiar situation of inadequate separation of duties. The same problem would exist where the machine operator had detailed knowledge of programs and had the ability to program. This situation also exists in some companies even where it is not required by a shortage of personnel.

Although limiting the machine operator's knowledge of detailed programs is a preventive internal control procedure, there are positive measures that help to detect irregular action. A console log would provide a record of computer utilization, the nature of stoppages, and summaries of errors or program changes that required operator intervention.

Some control must be maintained over these console print-outs, such as a locked copy of the print-out or prenumbered sheets. In addition, this console log must be reviewed by a knowledgeable independent party. Without proper review of the console log, there is no effective control.

A comparison of the actual time used with budgeted operating time, with variations investigated, would provide improved control. Any operator intervention would cause a substantial delay in processing that a review would detect. This control, however, could easily break down unless coupled with another preventive measure. There must be a standard procedure for each type of error that would cause a "halt" during processing. The operator's instructions in these circumstances should specifically indicate the error-correction procedures to be followed. The time and freedom available to the operator in the absence of written error routine instructions is a definite opening for fraud.

Programming fraud

An unusual example of a programming fraud illustrates the ingenuity of some of these people. This fraud took place in a bank and was committed by a machine operator. Ordinarily, operators did not have detailed knowledge of the computer programs, but this one was self-educated. By studying the program run book, he became familiar with the detailed computer instructions of the savings-account interest program that he wished to change. Thus, although the organizational plan limited the programming knowledge of operators, there was nothing to prevent the operators from gaining that knowledge on their own. The control system did not permit any opportunities for the operator to insert the fraudulent subroutine into the program for calculating and posting interest income to savings accounts, so the operator again used his ingenuity.

He purchased processing time at a computer service center and, with the addition of a fraudulent subroutine, duplicated the bank's interest program. Each savings account was credited with interest income as normally calculated, reduced by one dollar. These dollars were accumu-

lated and credited to the operator's account. The operator then carried the tape reel containing this fraudulent program into the computer room. Amid the confusion of processing deadlines, he insisted that the tape reel he had was the correct one and received little argument.

Input alteration

The machine operator can also cause an error by intentionally inserting a flaw in the input. One such fraud was committed by the manager of a cooperative computer center. The computer center manager inserted a "read flaw" on checks he wished to convert. Consequently, the altered checks were rejected during the entry run and were held for manual processing. The manager subsequently converted the checks to his own use. Although he did not change the computer system itself, the manager's actions placed chosen input documents in a vulnerable position.

The most obvious internal control procedure that would detect such an input alteration is the batch-control technique. Using this technique, a count of input documents is made when they are originally prepared, and this control total is compared with totals taken in various stages of processing. This procedure will not be effective unless there is positive follow-up and correction of detected differences. Unfortunately, there may be frequent differences between the original count and subsequent machine counts because of human error made in the first count. In this case, inadequate follow-up frequently results when differences due to faulty original count become a common occurrence. In addition, if a fraudulent input document is substituted for a legitimate input document rather than being merely added to the batch, the batch-control technique would not be effective. Unless input documents are prenumbered and accounted for, such substitution would be relatively easy.

Programmer

The programmers have detailed knowledge of computer operation and programming and would have the knowledge and ability to commit a programming fraud. If many programmers participate in the installation of a computer system, a fraudulent subroutine in the original program is unlikely since, with several people participating, the "debugging" of new programs would uncover the scheme. Since there are frequent alter-

ations of programs to adapt them to changing conditions, however, a fraudulent program change after the "debugging" is quite possible. A programmer would possess the knowledge necessary to make an unauthorized program change. He could also forge approval of a fraudulent program change. He could possibly add a fraudulent subroutine to a legitimately approved program change.

Internal control procedures aimed at preventing a fraudulent program change include requiring all program changes to be cleared through a person of authority other than through the programmer, documentation of the reason and effect of all program changes, and numerical accountability of change of program authorizations. If unauthorized changes are to be avoided, numerical accountability of change of program authorization is a necessity.

Programmers could also insert a fraudulent transaction into the records. Depending on the circumstances, either console intervention or alteration of input might be used to achieve this end.

An internal control procedure that could prevent alteration of the input or console intervention by the programmer is the organizational separation of the computer center and the systems and programming unit. In other words, programmers should be denied access to machine operations. Collusion between the programmer and the machine operator would combine the physical access to the records of the machine operator with the detailed knowledge of the system possessed by the programmer. The possibility of collusion would actually be the same as in a manual system.

Involuntary collusion

There is, however, a possibility of involuntary collusion that has aspects unique to a computer system. The machine operator might become the unknowing partner of a programmer in a fraud. If the machine operator has limited knowledge of programming and accounting matters, the programmer could give the operator instructions that would insert a fraudulent subroutine into the program or insert a fraudulent transaction into the data being processed. Insertion of a fraudulent transaction is particularly possible if the operator contacts the programmer when an error is detected during processing. Unless there is an established error routine procedure, the operator, by following the programmer's instruc-

tions, might allow the programmer access to the computer and to the records when a "halt" due to an error occurs. To avoid the possibility of involuntary collusion, the operators should be instructed not to accept instructions from programmers. Program documentation should not provide for instructions such as "See programmer in case of halt."

Systems Supervisor

The inherent authority in any supervisory position makes fraud and embezzlement easier. For a systems supervisor, the centralization in a computer system accentuates this problem. Combined with the knowledge and ability to make fraudulent program changes, the systems supervisor frequently has the authority to initiate such changes.

The most effective control for detecting a fraud by the systems supervisor is output sampling. A control group independent of the Data Processing Department would make an intensive verification of output on a sample basis. While this method would not detect all frauds, it would have a deterrent effect.

SPECIAL OPPORTUNITIES FOR FRAUD

Programming fraud will become a much more serious problem as authorization and approval for routine tasks become incorporated in the computer system. There have been suggestions that such decisions as writing off delinquent accounts, authorizing returns and allowances, approving invoices and preparing checks, reordering stock, and granting credit could be programmed into the computer. Writing off accounts receivable and reducing receivables for returns and allowances have been used in frauds and for concealment of defalcations. Putting authorization and approval of such decisions in the computer program means putting these decisions within the control of the personnel that control the program.

Manipulation of Master Records

The opportunities to change master records of many kinds deserve special mention. While such files as payroll, customer accounts receivable, and accounts payable were easily controllable when on ledger cards or the like, their transfer to computer device storage exposes them to ac-

cess by almost anyone in the EDP operation who can gain access to the programs, the magnetic tapes or disks, and a computer system.

The physical controls over these files must be tight. The authorizations for changes to master file information must be specifically assigned and always required. The computer programs that provide for changes to the master files should provide for printing a report showing: the master record before the change; the change made; and the master record after the change. This report should be closely controlled and forwarded to management personnel who can assess the propriety of the changes.

Departments initiating the changes should be furnished a copy of the report so they may determine whether the requested changes, and no others, were made.

Serious gaps in controls over master record changes have been noted in many installations, and this area affords an outstanding opportunity for fraud and embezzlement.

SUMMARY

It is continually amazing to note the sizable investment that many companies make in reaching a decision concerning computer feasibility, and then devote minimum, even token, attention to assuring that someone isn't siphoning off the assets by using the computer once it is installed. Unless the necessary controls are installed, the considerable time and effort devoted to determining the most suitable make, model, and color of computer hardware to be ordered, and the nature of the applications to be converted can constitute a great service to a potential embezzler by furnishing him the best system with which to achieve his objectives.

I am always suspicious of an EDP department that is "all loused up." The easiest way to steal in a data processing department is to do so poor a job that any possibility of fraud can be explained away as inefficiency or poor judgment. It seems to me that the easiest way to steal is purposely to develop a climate of chaos and then take advantage of it.

Over-all reviews of internal controls in the computer function must be thorough, well planned, regularly scheduled, and supplemented with special reviews as additional applications are converted. Additionally, periodic unannounced audits should be made.

The review must go far beyond mere questioning of the EDP man-

ager about whether such and such controls have been established and are in effect. The controls must be tested—tested by someone outside the computer function. One of the commonest control deficiencies found is that the controls described did not actually exist. Although management was assured that they were established, there were so many exceptions and so much laxity in their enforcement that they proved virtually worthless.

I am sure that many top management personnel are familiar with the matters discussed here and already have recognized to one degree or another the need to have these types of controls. But I will risk a good-sized wager that only a handful have a program for testing whether or not the controls described in the procedure manuals and job descriptions actually are being followed.

I strongly urge members of top management to take it upon themselves to obtain satisfactory assurance that the controls in the EDP function are suitably prescribed and actually are in effect. Test the system by attempting to put through inconsistent, unauthorized, or false transactions, or ask someone else to do so. Ask someone with whom EDP personnel are not familiar to try walking into the computer room and picking up reports, magnetic tapes, and programs. Test the follow-up over error listings and console typewriter messages.

In my view, the prime security measure in an EDP situation is an alert and informed management outside the EDP department. Management that is not informed on EDP control matters is at the mercy of their data processing manager, and those who fall in that category should understand this very clearly. If management does not understand EDP and cannot assess the controls surrounding that operation, or if they cannot take the time to do so, then they should obtain outside expert advice of persons who can perform this critical review and test function.

I hope that this discussion has contributed to a greater awareness of the risks involved in the EDP function and that you may feel prompted to test the presumed controls in your organization. In this way you may avoid appearing in future *Wall Street Journal* headlines that proclaim the sordid details of one of the major computerized embezzlements predicted by the experts.