115924

18930

NOMF

COMPUTER-RELATED FRAUD:

CURRENT ISSUES AND DIRECTIONS

Presented By

JAMES R. WATTS
GROUP DIRECTOR

ACCOUNTING AND FINANCIAL
MANAGEMENT DIVISION

U.S. GENERAL ACCOUNTING OFFICE

Before The

40TH INTERNATIONAL CONFERENCE
OF THE INSTITUTE OF INTERNAL AUDITORS

Phoenix, Arizona

June 8, 1981

82394

Computer Crime

Computer-related Fraud

Computer Abuse

By whatever name you call it--there are many, as we will see later--it is an intriguing subject. It is a topic on the agenda of many conferences being held this year. As a matter of fact, some conferences are devoted solely to this subject. People have written books about it and newspapers and various periodicals carry feature stories about it.

At the outset here this morning, I would like to look into some of the reasons.

WHY COMPUTER-RELATED CRIME IS AN ISSUE

In my opinion, several factors have caused it to be an issue of importance; the first, I like to call the "confusion factor." In part, this can be illustrated by some headlines and excerpts in newspapers and the trade press. For example, just last month one of Business Week's feature articles was "the Spreading Danger of Computer Crime." About 6 months earlier several newspapers reported that according to experts more people are getting away with and getting rich from computer crime. But it was just over a year ago that expert witnesses were testifying before the Congress that computer crime was a bogus issue, not significant enough to warrant passage of a Federal computer crime statute.

Confusion also surrounds the definition of computer crime. Many will say that the $10.2 million, wire-transfer, "diamond" fraud at a major California bank is a computer fraud; others say it is not.

Confusion also surrounds the magnitude of the computer crime. Some estimate that it is about $100 million a year; some say $300 million; some ever say it is in the billions. The truth is, nobody really knows because many cases go undetected for a long time which makes you wonder how many are never detected; and many of those which are detected generally are not reported publicly.

In addition to the "confusion factor" various legislative proposals make computer-related crime an issue of some significance. In 1977, Senator Ribicoff introduced his computer crime bill entitled "The Federal Computer Systems Protection Act of 1977." He introduced the bill, in part, because of three reports we issued in the mid seventies. Later, I will discuss one of those reports--the one on computer-related crimes in Government. The others addressed major weaknesses in computer security and faulty controls in major computer applications.

While the bill has not become law, several States have enacted their own. According to my last count, 11 States have passed computer crime statutes and several others are considering such laws.

Two other closely related factors make computer crime an issue worth reckoning with. One is the growing dependence of corporations and Government on the use of computer technology. The other is the growing pressure for the accounting and auditing professions to accept more responsibility for detecting fraud.

The computer dependency phenomenon has been creeping up on us. Many industries--banking, insurance, retail, manufacturing--are so dependent, they could not function very long without their computers; for others, its just a matter of time. Computer

dependency in the Federal Government is very high. Today, for example, we have over 18,000 computer systems in operation; compared to only a small handfull in the 1950's. As we all know, the size and scope of Federal activities has increased substantially, yet the Federal work force has increased only about 15 percent since the 50's.

With this increased dependence comes an increased exposure to the incidence to computer-related fraud. This is occurring at a time when audit responsibility for detecting fraud is receiving increased emphasis. In 1978, the Commission on Auditors' Responsibilities concluded that "All segments of the public--including the most knowledgeable users of the financial statements--appear to consider the detection of fraud as a necessary and important objective of an audit." The Report of the Special Committee on Equity Funding stated that the auditing profession should continue to improve its auditing procedures so it can increase the probability of detecting material frauds. Lastly, the Statement of Auditing Standards, Number 16, in effect tells the auditor to plan the audit to search for material errors or irregularities--that is, frauds.

So, on the one hand we have legislation being considered or enacted to address part of "the Problem," a push for auditors to better attack "the Problem," but, on the other hand, we have some confusion on the definition and size of "the Problem." During the rest of this session I propose to look at definitions, the legislative scene, and recent and on-going studies which address the security and audit implications of computer-related crime.

WHAT IS COMPUTER-RELATED FRAUD/CRIME?

Up to now I have used three or four terms somewhat interchangeably: computer crime, computer-related crime, and computer-related fraud. From now on I will use the later two terms, which I will define in a moment.

One author complied a list of over 20 terms which are used in the literature discussing this subject. Among others these include: computer abuse, computer capers, computer theft, computer-managed fraud, and programmer fraud.

Computer abuse is a commonly used term which has been made popular by Donn Parker of the Stanford Research Institute. He uses the term to describe

> " . . . any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator by intention, made or could have made gain."

He uses this term broadly to include computer frauds; destruction of computer hardware, software, and data; theft of software or data; and unauthorized use of computer time.

Computer-related crimes is the term we used in our 1976 report on such crimes in Government. We defined computer-related crimes to be

> " . . . acts of intentionally caused losses to the Government or personal gains to individuals related to the design, use, or operation of the systems in which they are committed."

This definition recognizes that computer based data processing systems are comprised of more than just computer hardware and software that run them. The system includes the organization and procedures--some manual--for preparing input to the computer

and using output from it. Thus, by this definition, computer related crimes may result from preparing false input to systems and the misuse of output as well as the more technically sophisticated crimes such as altering computer programs. It also includes the theft of computer time and software, as well as the destruction of software and data files.

Computer-related fraud is the term we are using on the AICPA EDP Fraud Review Task Force. We have defined this term to include:

> " . . . any intentional act or series of acts designed to deceive or mislead others. Such act must impact or potentially impact the financial statements and a computer system must be involved in the perpetration or cover-up of the scheme."

Please note that there are three essential elements in this definition. First, there must be intent to defraud. Second, there must be impact, or potential impact on the financial statements, and a computer system must be involved. The last element is the one which is usually the cornerstone of most debates over whether a fraud is computer related. Consequently, we have asserted that a computer system might be involved through improper manipulation of:

(1) input or transaction data

(2) output or results

(3) application programs

(4) data files

(5) computer operations

(6) communications, or

(7) computer hardware, systems software, or firmware.

The Task Force has specifically excluded from its definition the theft of software, hardware, or data as well as theft of computer time. The Task Force believes that such thefts do not have a direct impact on the financial statements.

Before I move on to the legislative scene, I would like to add a personal observation on devising a definition. We must recognize that we are dealing with a moving train. Computer technology is not standing still--it is moving ahead at ever-increasing pace. Also, the application of this technology to financial and general management systems is increasing in intensity and in sophistication. Therefore, it is very likely that schemes and methodologies for perpetrating and covering-up fraud in automated systems will also change. The way frauds were perpetrated 5 years ago may not be perpetrated the same way 5 years from now. Consequently, our definition must be flexible enough to accomodate these changes. In my opinion, the term "computer-related" does this quite well--it causes us to look at the general system in which the fraud was perpetrated, not just the computer itself. From an accounting and auditing point of view, our ultimate objective is to devise a system of internal controls which will help prevent and detect computer-related frauds; we cannot do this well by looking at the computer only.

WHAT DOES THE LEGISLATIVE SCENE LOOK LIKE?

So much for definitions; I would like now to turn to the legislative scene.

Over the last 4 years, Congress has been considering a Federal computer crime statute, but, as yet, none has been passed.

As I indicated earlier, Senator Ribcoff introduced his bill because of a growing national dependence on computers and the opportunities for white collar crime were becoming great; yet, at the same time, he was very concerned about the difficulties lawyers were encountering in prosecuting computer crimes under existing laws. He had learned, for example, that

--in one case, part of an indictment was dismissed because electromagnetic impulses which transmitted valuable data over a telephone line were determined not to be "property" as defined in the Interstate Transportation of Stolen Property Statute.

--in another attempted prosecution, the Government lost the case because of difficulties in establishing whether checks issued by a computer on the basis of fraudulent or manipulated data were forgeries.

Hearings were held on this bill in 1978 and again in 1980; however, the bill was never reported out of the Senate Committee on the Judiciary. Opponents of the bill argued--apparently with success--that the bill intruded into legal areas traditionally reserved for the States; and that many sections of existing law already provide adequate authority for prosecuting computer crime.

Even though the Feds have not passed a computer crime statute, at least 11 States have, and others are considering such laws. For the most part, these laws make the following acts criminal--most felony--offenses:

(1) devising or executing any scheme to defraud,

(2) stealing of data, software, or computer time, and

(3) altering, damaging, or destroying computer hardware, software, or data.

The computer crime statute in one State (North Carolina) makes it a misdemeanor offense to devise or execute a scheme to obtain a false educational testing score, or a false academic or vocational grade. Two States (Florida and North Carolina) also make it a criminal offense for any person to act willfully and without authorization so as to deny or cause to deny computer services to an authorized user of a system.

As you can see, these statutes are designed primarily to assist lawyers in prosecuting criminal cases which involve the use of computers. Most of us here, however, are more concerned about the auditor's perspective. And, I suppose the first thing that comes to mind is the Foreign Corrupt Practices Act. Well, I am not a lawyer, and I am not presumptuous enough to stand up here and attempt to interpret that one--we will have to leave that to the lawyers and a few test cases. I suspect, however, that the provisions in the Act dealing with internal controls would be a cause for concern because most of the computer crime cases I have analyzed were able to happen because of breakdowns in fundamental internal controls.

GAO Report on Computer-Related Crimes in Government

Several years ago, a now well-known individual began telling the world about the potential for computer crime, or abuse, and cited several cases. Oddly enough, none involved the Government. Based upon our experiences, we knew the Government could not be "Clean as a hound's tooth." If it was, it would be a first.

So we undertook a major effort to look into this obviously unusual phenomenon Our work confirmed out doubts: The Government is not unique; it, too, has its share of computer-related crime.

Our job was not easy because agency records did not simply say, "This is a computer-related crime." As I indicated earlier, such a definition recognizes that the computer is not the system, but is only a part, albeit an ever-increasing part.

In the final analysis, our primary sources for cases were memories of FBI agents, U.S. attorneys, the criminal investigator types in DOD, and audit and investigative groups in other Federal agencies.

When we checked out over 100 such cases, we found that not all were, in fact, computer-related, and our confirmed cases narrowed down to 69. When we analyzed these cases, we ended up categorizing them in four major groupings.

--Fraudulent input:	62 percent
--Unauthorized use of facilities:	26 percent
--Alteration or destruction of data files or programs:	23 percent
--Misuse of output:	17 percent

In the fraudulent input area, we have the case of a supervisory clerk who was responsible for entering claim transactions to a computer-based social welfare system. She found she could introduce fictitious claims on behalf of accomplices, and they would receive the benefits. She was able to process over $90,000 in claims (authorities believe it might have been up to $250,000) before she was discovered through an anonymous telephone tip. (Note: She was a system user, not a computer type.)

In the unauthorized use of facilities, we have the computer programmer who used the system to develop programs which he hoped to sell commercially.

In the third area of altering files or programs, we have the case of a transferred serviceman who--being familiar with an automated personnel system--used a terminal to alter his efficiency rating upward, and who was promoted on the basis of that high rating. Here, again, the discovery was a fluke.

In the misuse of output we distinguish between output which was generated from fraudulent input and ordinary legitimate output which was "gloomed on to" by an enterprising criminal. A case in point would be the selling of information on private citizens to special interest groups.

I'm not going to describe any more cases for you; you've probably heard enough "war stories." I think it would be more useful to look at these cases as a common body of knowledge and see what kind of generalizations we can draw from

it. I've identified several points; further analysis will probably reveal more. They are:

1. All types of systems were vulnerable: payrolls, accounts payable, welfare, inventory, etc.
2. Fraudulent input was a high vulnerability area.
3. The distinction of being a computer criminal was not reserved to computer-knowledgeable people. System users seem to be equally, if not more, common.
4. Perpetrators took advantage of system control weaknesses.
5. Weaknesses exploited were mostly basic management controls long recognized as being necessary to insure proper operations.
6. Most common weaknesses which were exploited were (a) separation of duties, and (b) physical control over facilities and supplies.
7. Sometimes these weaknesses were due to poorly designed systems, but in 7 of 12 cases we studied in detail, controls or procedures existed but were not enforced by operating personnel.
8. Computer crime detection was mostly accidental, not discovered by audit.

AICPA EDP FRAUD REVIEW TASK FORCE

It was against this back-drop in 1977 that the AICPA established the EDP Fraud Review Task Force. Donn Parker and our office were reporting on various cases of computer-related fraud; Senator Ribicoff and some States were introducing computer crime legislation; and the auditing profession was being told to do more to combat and detect fraud. There was also a recognition that the clients of CPA firms were becoming extremely computer intensive.

The Task Force met for the first time in 1978. It was composed of people from the auditing profession, academea, private industry, and the Government. The basic objectives of the group are to

--raise the awareness of the auditing profession to the incidence of computer-related fraud; and

--identify and propose controls and auditing procedures that will help detect and prevent computer-related frauds.

The specific tasks were to determine

--the kind of data needed for analysis, and

--where and how to get the data.

In carrying out the work, two major problems ensued. First, what is computer-related fraud? We solved this one fairly easily--we have a good working definition and it is serving our purpose quite well.

The second problem was more difficult to solve--we knew what kind of data we needed for analysis, but we couldn't get it very easily. We went to many sources: CPA firms, district attorneys, the FBI, industry trade associations, the Department

of Justice. They did not have the data we needed; in some cases (e.g. FBI) the data they had could not be released.

We finally hit upon a questionnaire approach to be applied on an industry-by-industry basis. The industry we selected first was banking because

--several cases had been reported in this industry by Donn Parker and the press;

--banks had a commodity that computer criminals usually sought--money;

--it is a heavy user of ADP; and

--it is heavily regulated and therefore required to report cases of fraud to regulatory authorities.

We also added members to the Task Force temporarily--the chief internal auditor of a major bank, a member of the FDIC, and a CPA who specializes in auditng banks.

We also sought and got the help and support of the Bank Administration Institute--the BAI has been one of the keys to the success of the study. All members of the Task Force are convinced that it was the joint sponsorship of the BAI and the AICPA which elicited the high level of cooperation we got from the banking industry.

The questionnaire was tailored to the banking industry--including banking jargon. It includes 34 questions--some with many sub-parts. It asks for information on who the perpetrator was, how the fraud was perpetrated and concealed, how it was detected, the degree of computer involvement, the existance and absence of controls, the degree to which audits were made, etc., etc.

Because of the sensitivity of the issue and the general reluctance to report frauds, we did not require the respondents to identify themselves. There is no way we could identify them unless they volunteered their identity--which was an option we gave them. Interestingly, about half of those who reported that they had had frauds and were willing to fill out the questionnaire, identified themselves.

We sent the questionnaire to all 9,000 (plus) banks which are members of the BAI. This gave us excellent coverage of the banking industry which is composed of over 14,000 banks. We also sent a follow-up request to the top 1,000 banks of BAI. This, of course, had to be sent blind because we did not know who had responded to the first request.

Over 5,100 banks responded to the questionnaire, a response rate of about 57 percent. Of these, 105 banks reported at least one case of what was believed to be computer-related fraud; a few banks said they had more than one case. After reviewing the cases in detail and following up with those who identified themselves, we have reduced the number of cases to 85. Some did not meet our definition; for others, enough data was not available to make a judgment.

What I would like to do now is to step through several slides which summarize some of the data on the 85 cases. But first, let me throw out a couple of precautions. First, these are preliminary statistics. We are still re-checking our analyses and some of the figures may change by a point or two. Second, do not attempt to project this data to the banking

industry--there are biases in the universe whose significance cannot be evaluated statistically. For example, it is believed that many frauds go undetected--we don't know the effect of that; there is the reluctance to report--we do not know the effect of that either. Also, we still have the problem of definition--two banks told us they disagreed with our definition and were not going to participate.

On the positive side, however, we do have a very good picture of the nature of computer fraud in these 85 cases. They can be good indicators of vulnerable areas and things to look for and possibly concentrate on.

Applications

1. 16 applications systems were hit.
2. About half were in checking and savings.
3. Five applications account for over 77 percent.

Perpetrators

1. Clerks and proof operators accounted for 46 percent; these run the gamut from;
   - --removing items from processing,
   - --forcing rejects and reprocessing to other accounts;
   - --changing due dates on peronal loans,
   - --increasing personal credit limits.
2. Managers: these were mostly loan officers.

Scheme

1. Scheme: basic type of artifice or ploy used to perpetrate the fraud--16 different ones in all.

2. Fictitious loans--actually the loans were "real" in several cases, just unauthorized. For example, a Charge Card loan officer set up several unauthorized charge accounts on the master file and set very high credit limits. The officer would put in time extensions to avoid past due accounts; at other times he would destroy past due reports; $50,000 over a 15-month period.
3. Diversion of deposits.
4. Deferral of posting checks.
5. Increasing Credit limits.
6. Forgery: computer operator encoded checks with numbers of closed accounts. Accomplice cashed them. Operator interupted them and returned them unpaid because the accounts were closed.

Method Used

1. Methodology refers to the way the computer system was manipulated:
   a. file maintenance
   b. transactions
   c. access inquiry (media)
   d. programming
   e. direct file changes
2. File maintenance--most non-financial
   a. increasing credit limits
   b. changing due dates on loans
      --Example: unauthorized extension of due dates on $1 million in loans; $250,000 proved to be uncollectible; motive not clear, but probably to hide poor performance in collection.

c. changing date of last payment

d. reactivating closed credit or loan accounts with altered addresses.

3. Transaction manipulations

a. to force rejects

--Example: Encoding altered to force rejects; typically perpetrator had access to rejects. Bookkeeper changed one of the MICR digits on his checks; cashed the check; and destroyed the rejected item.

b. to divert deposits

--Example: Proof operator found deposit ticket failed to include one check, so added it to his own account; it worked! He became bolder and began removing deposits from customer accounts and added to his own. Went on for 7 months.

c. Diversion of receipts

--misencoding rejects during reprocessing

d. Creating original items

4. Access to media--had access to ATM card of customer; stole card from the bank; used terminal to obtain PIN and used card to make unauthorized withdrawals.

5. Direct file changes

a. Applications programmer used a utility program to transfer funds to his savings account from account of customer.

b. Used software program to decrease balances in inactive savings accounts and increase balance of his own account.

Prepared falsified statement to customer; was revealed when Post Office return falsified statement; customer came in, asked for his statement; got a current one and questioned it.

How detected

1. Concerns about money
   --reluctant to disclose because of tendency to say this is average size of computer-related fraud--this is misleading; could be used to over dramatize or underdramatize and misdirect attention away from other lessons to be learned.
   --reluctant not to disclose because might be accused of withholding information.
2. Twenty-nine cases (1/3) detected by audit and internal control. Eight of 12 detected by internal controls were detected 4-12 months after first initiated.
3. Twenty-four cases (1/3) detected by customer complaint (mostly in first 3 months). Reinforces role of customer as key element of control.

General Observations

Many observations can be drawn from this data; as a task force we are still doing this, but here are some for starters:

1. The customer is still a major control element for identifying problems. Consequently, controls over developing and mailing customer statements are very important.
2. Many perpetrators used their own accounts to extract funds; therefore, special controls and extra audit of employee accounts may be in order.

3. Loan officers frequently used fictitious loan schemes to perpetrate fraud. Therefore, enhanced control over loans might be in order--e.g. reporting new loans and maturity extensions to higher management.

* * * *

We are now refining our analysis of the data and developing observations. We have a tight time schedule ahead of us--we are hoping to get a final draft approved in September; and publish a research paper and article in the Journal of Accountancy soon thereafter.

At this time, we are also working hard on a comparable study of the insurance industry. In early April we mailed an insurance version of the questionnaire to over 1,200 insurance companies. The questionnaires are just now coming in and we will be publishing a separate research paper on those cases. We ultimately hope to survey several industries and issue separate reports on each. Later, we propose to summarize all industries pointing out common results.

In closing, I would like to request any of you who may be lucky enough to receive one of our questionnaires to fill it out if you have any cases of computer-related fraud. I am convinced that this is the only way for us to eliminate some of the confusion that surrounds this area.

Thank you.