1893/

COMPUTER-RELATED FRAUD: CURRENT ISSUES AND DIRECTIONS

115925

Presented By

JAMES R. WATTS
GROUP DIRECTOR

ACCOUNTING AND FINANCIAL
MANAGEMENT DIVISION

U.S. GENERAL ACCOUNTING OFFICE

Before The

SIXTH AICPA NATIONAL
CONFERENCE FOR
CPAs IN INDUSTRY

Atlanta, Georgia

MAY 7, 1981

017653

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 even 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 an 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 <u>system</u> of internal controls which will help prevent and detect computer-related frauds; we cannot do this well by looking at the computer only.

<u>WHAT DOES THE LEGISLATIVE SCENE LOOK LIKE?</u>

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.

I think most of these points have a strong message for the auditor; namely, he/she must become actively involved in ADP system controls. After all, an effective system of internal control is highly dependent upon an effective system of audit and internal review.

GAO Computer Audit Standards and Objectives

For some time now, our office has been concerned that the audit coverage of computer-based systems does not measure up to the quality needed. Consequently, we have established two standards for auditing computer-based systems. These standards apply to auditors who audit governmental organizations, programs, activities, and functions.

The first standard is:

> "The auditor shall review general controls in data processing systems to determine that (a) controls have been designed according to management direction and legal requirements, and (b) such controls are operating effectively to provide reliability of, and security over, the data being processed.

Under this standard, auditors are to review and evaluate general controls and consider their effectiveness in reviewing individual application controls. The auditor should review the organization, delegation of authority, responsibilities, and separation of duties in the organization; also, the adequacy of the physical facility, personnel policies, and security, as well as operating system and hardware controls.

The second standard is:

"The auditor shall review application controls of installed data processing applications to assess their reliability in processing data in a timely, accurate, and complete manner."

The basic objectives of this standard are

--to determine whether the installed application conforms to standards and the latest approved designed specifications, and

--to disclose possible weaknesses through periodic audits designed to test internal controls and the reliability of the data produced.

We also feel very strongly that the auditor must fulfill certain responsibilities during the design and development of automated systems. Consequently, we have also established the following audit objective:

Review the design and development of new data processing systems or applications, and significant modifications thereto.

Please note that this is an audit objective, not a standard. We recognize that compliance may not always be feasible because adequate resources and audit skills may not be available. Also, internal auditors may need additional specific authority from management to do this work.

The objectives of requiring auditor review of system design, development, and modification are to provide reasonable assurance that systems/applications;

1. carry out the policies management has prescribed for them;
2. provide the controls and audit trails needed for management, auditor, and operation review;
3. include controls necessary to protect against less or serious error;
4. will be efficient and economical in operation;
5. conform with legal requirements;
6. are documented in a manner that will provide the understanding of the system required for appropriate maintenance and auditing.

NBS Report on Safeguards Against Computer Misuse

Before I give you a status report on the AICPA EDP Fraud Review Task Force, I would like to refer you to a couple of reports which you should find useful in looking at what policies and strategies you might want to establish in your corporation to combat the potential incidence of computer-related fraud. Both reports are based upon many of the cases of computer abuse which have been researched by Donn Parker at the Standard Research Institute.

The first report was prepared in 1978 by the Standard Research Institute for the National Bureau of Standards. It is called "An Analysis of Computer Security Safegards for Detecting and Preventing Internal Computer Misuse."

Please note, if you will, that my dear friends at the Bureau of Standards, who are in the business of what? --setting standards abviously! --did not adopt one of the more commonly used terms like computer crime, or computer abuse. Instead, they came up

with yet another term--unintentional computer misuse! Essentially, it means the same thing as the terms computer abuse and computer related fraud, but they also use different words. This new definition is: an intentional act directed at or committed with a computer system or its associated external data or program activities in which there is:

1. unauthorized modification, distruction, or disclosure of intellectual property (data or programs);
2. unauthorized modification, destruction, or theft of physical property (equipment or supplies), or
3. unauthorized use or denial of a computer service or process.

I had better let up a little on these innuendoes, otherwise you are going to wonder why I am suggesting this as a reference source. In defense of NBS, the report was written for a computer security specialist. Essentially what they have done is develop what they call a taxonomy or list of vulnerabilities and cross-indexed them to a set of 88 safeguards (or controls which will help detect or prevent a perpetrator from taking advantage of an automated system or commit an unintentional computer misuse or crime!

O.K. Here is a partial list of these 17 vulnerabilities. You can get the idea of the missing ones, however. For example, the 2nd and 3rd ones are unauthorized destruction and unauthorized disclosure.

You might be wondering a bit about programs external to the computer system. They are talking about programs stored on cards or those stored on tape or disk but modified on another computer system.

I suppose I should have put up "Denial of Computer System Service" the students, as we discussed earlier, are having fun making this one popular.

O.K. Now for the safeguards - here are a couple of examples. Name is pretty obvious; Category means who "organizationally" is responsible for instituting and maintaining the control. In this case they mean data handling in the operations or user department. Description is self explanatory--I picked this one because it is fairly important in preventing a number of computer related frauds. Purpose is the cross index to the vulnerability; and finally comments - retrofit means that if the control had been left out in the original design then it can be installed without too much difficulty.

Here's another example. Here, internal control means the internal control group with the data processing department.

Department of Justice Manual
for Criminal Investigators

Now, while this report, was targeted for the computer security specialist the other report in designed for criminal investigators. But it also has alot of good information that internal auditors would find useful. The report is "Computer Crime, Criminal Justice Resource Manual" and was prepared for the Department of Justice by the Standard Research Institute.

At the outset, let me tell you that it is nearly 400 pages long--so I'm only goint to touch on a couple of things.

The manual has a section on

--definitions and history of computer-related crimes and discussion on the technical jargon of computer crime methods/techniques such as data diddling, superzapping, logic bombs, etc.;

--experts, witnesses, and suspects;

--legal definitions of computer technology, and evidence considerations;

--computer-related crime laws on Federal and State levels; and

--an overview of computer technology.

There are two sections in the manual which I think you might find useful from an audit point of view.

First, the report includes an analysis of 362 recorded cases of computer abuse showing common functional weaknesses.

Here we can see again that manual handling of input/output data is a high vulnerability area.

Four of the cases under "physical access to EDP facilities" involved attacks on computers with forearms. Two of these are presumed to have involved citizens frustrated in dealing with Government bureaucracy and computer-based services.

For each of these areas, there is a very general description of the types of crimes committed followed by a history of the controls that were found to be weak or nonexistant.

Another useful part of the manual for audit is an analysis of occupations which pose varying degrees of risk to a company for the perpetrator to computer-related crime. Take note of who is at the top of the list. It is assumed in the analysis that good controls are in place and functioning. Obviously, if controls were not in effect, the risk would be higher.

For each of these occupations, the manual includes the following descriptions:

--here's the auditors, for example--

--functions

--knowledge

--skills

--access

--vulnerabilities

--conclusions.

AICPA's EDP Fraud Review Task Force

Another initiative to combat computer-related crime is the AICPA's EDP Fraud Review Task Force. The Task Force was established in May 1978 for the purpose of

(1) raising the awareness of the auditing profession to the incidence of computer-related fraud, and

(2) identifying and proposing controls and auditing procedures that will help detect and prevent computer-related frauds.

The general membership of the task force is composed of people from academia, auditing firms, private industry, the FBI, and GAO.

fraud in the industry and to identify which controls were commonly compromised and what auditing techniques would be the most effective in detecting and preventing such cases of computer-related fraud.

The first industry we have selected is banking, primarily because most of the published cases of fraud have involved banks. To make sure our task force has the proper mix of background and experience, we have temporarily added to the task force a CPA who specializes in bank audits, the chief internal auditor of a major bank, and a representative of the Federal Deposit Insurance Corporation. These people will be replaced by people from the next industry we select for study.

To obtain the information we need from the banking industry, we have developed a questionnaire which will be sent to about 9,000 banks next month. The questionnaire is being mailed to the chief internal auditor of each bank. The questionnaire is jointly sponsored by the AICPA and the Bank Administration Institute which is a permanent member of the Task Force.

The questionnaire asks each bank to disclose whether it has had a computer-related fraud and specific details on any such case of fraud. The task force is very much aware of the sensitivity of such a request. There is a natural and understandable reluctance to disclose such incidences outside the bank. Consequently, we have designed the questionnaire and the procedures for distributing it to assure complete anonimity.

There is no way any member of the task force or anyone else will be able to identify a questionnaire to a specific bank.

After we have received and analyzed the returned questionnaires, we will publish a report that will discuss a composite profile of computer-related fraud in the banking industry.

Some of you out there may in fact be employed by banks; in which case you are very likely to receive the questionnaire. Please take the time to fill it out and send it back to us. The instructions on the questionnaire explain in detail our definition of computer-related fraud; if you are not sure whether your case or cases fit, fill out the questionnaire anyway and tell us that you are in doubt. If you give us enough particulars, we'll be able to decide.

As far as we know, this is the first attempt ever to systematically and scientifically determine the incidence and nature of computer-related fraud in any industry. The results of the study could put to rest many of the unknowns and issues that are frequently debated in conferences such as these.