1991

Computer crime: The abuse of accounting information systems

Darin J. Anderson
University of Northern Iowa

Presidential Scholars Senior Thesis

Computer Crime: The Abuse of Accounting Information Systems

by

Darin J. Anderson

Advisor: Professor Ron Abraham

Prepared for:
Presidential Scholars Board
Myra R. Boots, Chair

Abstract

This thesis will explore the impact of computer crime on accounting information systems. Specifically, it will address the different types of crimes committed, the types of people who commit them, and the controls to deter them. The paper will then close by focusing on who should take responsibility for detection of such crimes.

May 23, 1991

Introduction

As we sit here in the latter part of the twentieth century, we find ourselves riding the crest of the computer revolution, swept along by advancement after advancement. Indeed, the strides made in computer technology and the application of this technology to our everyday lives in the last half of this century have been staggering. Even more staggering is the fact that this revolution is continuing, and the computers of the next century will have capabilities that we wouldn't think remotely possible today. The computer is truly here to stay, evidenced by its pervasiveness in our everyday lives. The society of the early 1990s sees computers being used in education (at earlier and earlier levels each year), physics, aerospace technology, sports fitness, and nearly everywhere else.

One need only look at the recently completed Persian Gulf War to see just how far computer technology has taken us. The computerized airplane cockpits and computer-guided missiles, which allowed removal of military targets with such precision as to keep civilian casualties to a bare minimum, serve as spectacular examples of how far we have come in this area. But perhaps the most common uses for computers today lie in the areas of data storage and manipulation, lending themselves to widespread use in bookkeeping and accounting applications.

In these areas, especially, the computer has greatly increased the efficiency of accountants by relieving the of the tedious task of data processing (i.e. adding, multiplying vast amounts of numbers), thus allowing them to better serve

management as analysts and prognosticators. Due to the impact of the computer age, the accountant serves a greatly different role than in previous decades.

However, the advent of the computer system has proved to be a double-edged sword. While relieving much of the tedium of accounting work and increasing efficiency of the data processed, these computerized systems also lend themselves to abuse. This susceptibility to misuse arises from the distortion of the audit trail, which is a trail of records allowing accountants to trace the flow of financial information through the accounting system from the beginning source documents to the resulting financial statements. In computerized systems, this trail is maintained almost entirely within the computer, leaving little or no "hard" paper documentation. This makes it difficult to trace transactions through the system, and thus makes it easier for people with the proper knowhow to conceal wrongdoing.

Since the computer era is relatively young, there has not been a great deal of attention directed to the specific area of computer crime involving accounting information systems. Since the computer is a permanent feature of our society, however, I think you will see this becoming an issue of central concern in the years to come. The purpose of this project is to examine how such crime is perpetrated and how it may be deterred.

Scope of the Problem

Frequency of Computer Crimes

To begin the examination of this problem, it is helpful to look at the statistics currently available regarding computer crime. Perhaps the most notable thing about these statistics is their absence. Since the first commercial computer was introduced in 1950, only around 2000 cases have been discovered (Moscove and Simkin, 1987, p. 329). By itself, this may seem like a large number. However, given that there are over 200,000 computers in use in the United States, alone, this number is surprisingly small.

There are at least two reasons for surprising absence of statistics. First of all, companies are extremely reluctant to discuss this matter. This shyness stems from the belief that discussing such activities will damage the reputation of the company. Because of this belief, most companies are more willing to handle such matters internally, where they can keep it quiet, rather than reporting the incident and letting the story be detailed in the media. Additionally, companies do not report computer crimes because of a phenomenon known as the skyjack syndrome. This syndrome arises from the fact that computer crimes are innately appealing. When such stories are reported, the publicity actually encourages such activity, rather than discourage it. Therefore, companies take a very defensive and quiet position when this issue is raised.

The second reason for the lack of statistics is that most cases simply are not

discovered. Many computer-related crime are being committed each day without being unearthed. It is estimated that only fifteen percent of all computer crimes in this country are detected. Of those, only five percent are made public, with a mere three percent being prosecuted (San Segundo, 1985, p.47). This is undoubtedly the biggest reason for the sparsity of reported cases, and it results from the fact that the nature of this type of crime is exceedingly difficult to detect.

Public awareness of this issue is on the rise, however, resulting in an increasing number of cases being made public. Simply comparing the number of stories of computer crime appearing in newspapers and magazines before 1988 with those appearing after 1988 shows a tremendous increase in the awareness of this issue and a related increase in the scope of the problem.

Even though there are relatively few documented cases of computer crime, there is still strong reason to believe that such crimes are being perpetrated in large numbers on a daily basis. This assumption is supported, first of all, by the huge growth in the number of computers being used, a number growing almost exponentially. This growth in the raw number of computers greatly increases the likelihood of these types of crimes.

A second reason to suspect that computer crime is running rampant today is the fact that no computer system can be one hundred percent fool-proof. Most systems do have at least a minimum number of safety features designed to dissuade criminals. But these systems controls are designed by humans, and humans can't

conceive of *every* possible way in which the criminals will circumvent the controls. Thus, until the perfect computer can design the perfect system, there will always be an inherent susceptibility to misuse.

A final factor supporting the assumptions about the scope of unreported crime is the fact that people are becoming less and less afraid of computers. Today, there are two types of computer users: those who are physically frightened when using a computer and feel they will destroy the world by pressing the wrong button, and those who embrace computers and see them as a powerful tool to accomplish any task before them. There is a dwindling number of the former and an increasing number of the latter types of individuals. This trend arises because people are leaning to use computers at an earlier age, making them feel more comfortable around computer terminals. Additionally, there are numerous classes and seminars being offered to teach people how to work with computers. The result is that people entering the workforce today have more knowledge and less inhibition about computers. Therefore, they are more confident about tampering with the system and attempting to manipulate the information contained therein for their personal gain. Donn B. Parker, a computer crime expert at the Stanford Research institute, stays, "I have studied more than 100 cases of computer crime. If all we're doing up to now is accidentally stumbling onto these things, I can't help but wonder what the really smart computer crooks are doing," (Dallos, 1975, p. 144).

Cost of Computer Crime

The frequency of occurrence of these crime is only half of the problem. Additionally, there is a high cost associated with each crime. The accounting firm of Ernst and Whinny (now Ernst and Young) estimated computer fraud losses in the United States at over three billion dollars in 1987 (Kneale, 1987, p. A22). This is not a problem unique to the United States, however. Britain, for example, lost an estimated seven hundred million dollars to computer crime in 1985. Moreover, the cost per crime is also very high in this area. While the average cost of the conventional bank robbery is $6,600 per crime, computer crime averages nearly $220,000 per crime (San Segundo, 1985, p.47).

Given the foregoing circumstances, it seems only logical to conclude that computer crime is an existing problem that, if left unchecked, could reach epidemic proportions in the years to come. The increasing frequency, coupled with the enormous cost associated with each crime, poses a serious threat to business and commerce all over the world. Therefore, immediate and serious attention needs to be directed towards this area.

Computer Crime Cases

Having seen that computer crime is an existing and growing problem, we can now explore some of the more "famous" cases of computer crime to illustrate how these crimes are perpetrated and the damages they can cause.

Equity Funding Corporation of America

The first and most well-known case of computer crime is the Equity Funding Corporation of America case. There is some degree of controversy as to whether this is a true case of computer crime. Some people argue that the computer was only a tool in this caper, and that this crime would have been committed whether a computer was present or not. However, since a computer did play a central role in this crime, and given the large dollar amounts involved, it seems appropriate to classify this in the computer crime area.

Equity Funding Corporation of America (EFCA) was a company in the business of selling insurance policies and mutual funds. The programs EFCA offered involved a very complex series of transactions, making it easier for the company to conceal the fraud. Participants in the EFCA programs signed up for ten-year installments, whereby the individual would purchase various mutual funds and then pledge these funds as collateral for loans from EFCA. The proceeds from these loans were then used by the participants to purchase life insurance from EFCA.

From the outset, EFCA adopted an aggressive growth strategy. To achieve

this growth, the company strived to generate high earnings. These high earnings, then, would raise the price of EFCA's stock being publicly traded. The higher stock prices would then generate more capital for the company to use in acquiring other, smaller companies, thus achieving their growth objective. High earnings was therefore the cornerstone of the Equity Funding corporate philosophy, and the company was quite successful in generating these earnings in the early years. However, the stock prices failed to respond in a favorable manner in later years, and EFCA turned to fraud to inflate their earnings.

The plan of deception actually consisted of three separate phases beginning in 1959 and spanning more than ten years. The first phase consisted of merely overstating revenues by creating fictitious mutual fund policies and recording commissions on the false loans supposedly taken out on these funds. When this didn't generate enough earnings, the company turned to the second phase of the plan, which involved acquiring several foreign subsidiaries. The company accountants then began transferring assets to and from these subsidiaries in a complex manner, so as to allow the same assets to be counted two or three times at.

When even this didn't produce the desired increase in stock prices, EFCA turned to the final and most confusing stage of the scam. This third phase utilized a quite legal practice of coinsurance, which allows one insurance company to sell its policies to another insurance company, with the selling company maintaining physical custody of the policies. Utilizing this technique, EFCA sold its fictitious

insurance policies generated in the first phase of the scam to other insurance companies. However, as is the common practice, EFCA was allowed to maintain custody of the policies and be responsible for keeping the records on these policies, thus affording EFCA all the opportunity it needed to conceal the fraud.

By the end of the scam, EFCA had created and sold more than 65,000 fictitious insurance policies. They were able to pull this off by utilizing a computer to manipulate the computer-stored records of these policies. EFCA assigned special account numbers to the fictitious policies and then programmed the computer to ignore these policies when the independent auditors asked for a printout of policies to ascertain their existence. Quite ingeniously, EFCA also periodically "killed off" some of the false policies to make the scam seem more realistic. It is estimated that fifty to seventy-five EFCA employees knew of this plot in some way or another. When the scam was made public, nine men resigned, and twenty-two people were indicted (Andrews, et. al., 1977, p. 3).

Another factor helping Equity Funding achieve such a high degree of success in this plan was the fact that Wolfson, Weiner, the independent auditors assigned to audit EFCA, were incompetent and computer-illiterate. In fact, Julian Weiner had been sued by various clients on many occasions. Additionally, Soloman Block managed the EFCA audit for four years, but was not even a C.P.A. at any time during this span. The independence of this firm was also in question as Marvin Lichtig, one of the accountants, later became an officer at EFCA, and Block's son

was on EFCA's payroll. These three individuals were later indicted on charges of fraud.

So incompetent was the Wolfson, Weiner firm that one of the co-insurers, Ranger National Life, asked *their* auditors (Peat, Marwick, and Mitchell) to audit EFCA. In fact, the Peat Marwick auditors came extremely close to unveiling the fraud. They found many irregularities that they were going to make public, but EFCA, through crafty legal maneuvering, had the Peat Marwick auditors thrown off the case.

The losses stemming from this case are astronomical. It is estimated that the direct losses from EFCA's activities are in the neighborhood of $200 million, while indirect losses (legal costs, declines in stock prices, etc.) may have reached as high as $2 billion (Moscove and Simkin, 1987, p. 335). These figures make the EFCA case the single largest case of computer crime, dollar wise, known at this time.

As previously mentioned, this particular case developed over more than ten years, and it could have gone on much longer if not for mere chance. This crime was discovered, not by extensive controls or by scrupulous investigations, but rather by a tip from Ron Secrist, a disgruntled employee. Secrist was a vice-president at EFCA and knew first-hand of the fraud. Citing an employee cutback, EFCA fired Secrist. This so angered Secrist that he then went public with the story.

TRW Credit Data

A second case of computer crime involves the TRW Credit Data company. This company offered credit data on various individuals to clients who depended heavily on this type of information, such as Sears, Mastercard, and other credit businesses. As would be expected, the voluminous amounts of credit information were stored in computer files to facilitate processing and updating.

Within TRW, a group of six employees came up with the idea of selling "clean ratings" to individuals whose credit ratings were tarnished. These six conspirators would contact the individuals and offer them a clean bill of health for a small "processing fee". These TRW employees would then access the records and either add new information to the existing records or delete the existing information to create a more favorable rating.

This case illustrates that physical assets are not the only things susceptible to misuse in a computerized system. In this case, valuable information was the target of the fraud, not cash or inventories. Clearly, computer systems contain much more than a mere record of assets; they contain a massive amount of vital data which can be misused in any number of ways.

The TRW Credit Data fraud, in like fashion to the Equity Funding case, was discovered only by chance. One of the customers who was contacted about changing their credit rating realized that this was illegal and took offense to the

solicitation. This individual then reported the act to the authorities, and the case was uncovered (Moscove and Simkin, 1987, pp. 339-341).

Lawrence Berkeley Laboratory

The preceding cases illustrated the abuse of accounting information systems for the purpose of monetary gain. However, some computer criminals misuse computerized accounting systems only as a means to a much larger end. A spectacular illustration of such a case took place in August of 1986.

Clifford Stoll was an astronomer working at the Lawrence Berkeley Laboratory (LBL) in California. He had worked there for many years, but the laboratory was finding it tough to utilize him on projects. Instead of simply letting him go, LBL decided to make him systems manager of their computer system. Stoll was by no means a computer wizard, but figured he could learn the operations quickly and accepted the job.

LBL's computer system consisted of a couple of mainframe computers. These mainframes were used to sell computer time to various physicists to run physics programs and to perform difficult computations. At the time, the LBL accounting program was a patchwork of many badly written and modified programs. In fact, it was written in three separate computer languages. Additionally, there was no documentation for this system, making it difficult to trace any kind of error.

After a couple of weeks on the job, Stoll noticed a 75 cent error in the

accounting records between billings and user time. Stoll brought this to the attention of LBL management, but they seemed unconcerned. Stoll suspected an error in the program, and figured that by finding the error, he would learn how the system worked. Stoll then traced the transaction through the programs, but, surprisingly and despite the patch-work nature, found them to all be working properly.

Stoll then dug deeper and found an unauthorized account in the computer records. LBL records contained only general, unclassified information, unlike some other laboratories in the area, which contained classified information about government and military activities. Because the LBL records were unclassified, Stoll suspected a small-time prankster or a student and deleted the account, figuring that would be the end of the intruder. But a few days later, the intruder returned, made a new account, and again tried to cover up the accounting records. Upon this second intrusion, Stoll and LBL decided to start monitoring this individual. To do this, LBL attached printers and alarms to various connecting ports which recorded every keystroke entered by the intruder. Ironically, this monitoring process revealed several other attempted break-ins to the system *completely unrelated* to the individual in question.

Stoll and LBL were very careful not to alert the intruder to their knowledge of his access. To this end, LBL refrained from discussing this issue in the electronic mail, and also sent false messages to make the intruder think he was not suspected.

Through his constant monitoring, Stoll found that the intruder was using the LBL system to leapfrog to other networks and that the intruder showed an interest in military information. At this point, Stoll involved the F.B.I. due to the international implications of the case.

With the assistance of the F.B.I., Stoll continued to monitor the intruder, and eventually traced the individual through various defense contractors and military installations to Germany. At this point, the BKA, the German equivalent to the F.B.I. also became involved. The combined efforts of these groups were finally able to pinpoint the intruders in the city of Hannover, but since the intruder never connected for more than a few seconds at a time, they couldn't trace the signal to any particular phone.

Stoll and LBL then created fictitious files in the LBL system discussing how computers were supporting SDI research in the United States. These were lengthy files which made the intruder connect for longer periods of time to read them. A few days after these files were entered into the LBL system, the laboratory received a letter asking for this particular information. The astonishing thing about the letter was that it was sent from *within the U.S.* This led the parties involved to suspect espionage. A complete investigation followed, and the members of the spy ring, both in the U.S. and Germany were apprehended. The names of the parties involved have been withheld pending litigation (Stoll, 1988).

The intruder in the LBL system was very careful and tried not to cause any

harm to the records in the system. Therefore, the direct damages from this case appear to be relatively small, estimated a around $100,000. Most of this amount results from stolen computer time and false phone calls. However, the intangible cost associated with this case could have been much greater. At one point, the intruder entered a computer used in the real-time control of a medical experiment with a human patient. Though no damage was done, the patient could have been severely hurt. Additionally, the information this espionage ring could have collected could have been devastating to the military efforts of the U.S.

In this case, a 75 cent error led to international espionage. The perpetrator had no intention of altering the accounting records to make a profit, but was merely trying to access another system for information. This intrusion probably wold have not been discovered had an astronomer been placed in charge of the computer system.

The Chairman and His Board

Yet another case of computer crime took place in the 1st National Bank of Chicago in May of 1988. The mastermind behind this plan was a man named Armand Moore, nicknamed "The Chairman". The key figure in the plan was Gabriel Taylor, an eight year employee of the bank with no prior record. Taylor was a clerk who was involved in multi-million dollar transfers between corporate accounts around the world.

Moore, after being paroled in 1986 for fraud, was introduced to Taylor by

Moore's cousin, who also worked at the bank. Moore had conceived plan to divert corporate funds to his private bank account. It was 1st National's policy to callback the executives of the companies after they requested a transfer and obtain pre-established authorization codes to ascertain that it was a bona fide request. This process was also taped for security reasons. Taylor, as a trusted employee, was given access to these codes.

Moore's plan commenced on the morning of May 13, 1988. Per Moore's instructions, several of the other members of this ring called Taylor requesting transfers in the names of United Airlines, Merill Lynch, and Brown Foreman (maker of Jack Daniel's whiskey). Taylor then called back the gang members using the stolen codes. Transfers in the amounts of $24 million from Merill Lynch, $20 million from Brown Foreman, and $25 million from United Airlines ($69 million in all) were sent to fictitious accounts in Vienna, Austria. The plan took only 64 minutes to execute.

As with all of the preceding cases, this case, too, was only discovered by luck. The only thing that alerted bank officials to this crime was the fact that United and Merill Lynch didn't have enough funds left in their accounts to cover outstanding checks. When these checks started bouncing, the bank officials became suspicious and called the F.B.I. Even though they were caught, this ring came very close to pulling the scam off. Said one investigator, "They came a lot closer than the banks want to acknowledge," (Boch, 1988).

More Common Cases

While the previous four cases serve as rather spectacular examples of how computer systems can be misused, they are by no means the everyday type of crimes. They only happen once in a while when a special person is given a special opportunity. The more frequent cases involve techniques known as lapping of accounts receivable and the round-off trick.

Lapping of accounts receivable arises when persons in charge of receiving customer remittances pocket the money and then use subsequent remittances to conceal the crime. After they convert the first check, they will then apply the next remittances to the account which was supposed to be paid with the stolen money. After the first account is covered, they apply the remittances to the next account, and proceed in domino fashion through the rest of the accounts.

Typically, the first purchases and billings are the first to be remitted. Therefore, customers who send payments near the end of the month may not complain if their accounts are not credited, because they figure the check as not been processed when the money has actually been taken. By the end of the next month, enough money will have been received to cover these accounts, and the customers will never complain. Lapping is a technique that can be utilized in both computerized and manual systems, but the computerized environment makes it much easier to conceal such activity.

The round-off trick is unique to computerized systems. This technique is

used in processing payroll amounts or in calculating interest on deposited amounts. Computers usually figure calculations to fifteen digits, but currency can only be payable in two decimal places. The computer must then round off the calculation to the nearest cent. The round-off trick involves reprogramming the computer to always round down and to then send the remaining fraction of the pay to a specified account.

This is a very effective technique because it is hard to detect, due to the small dollar amounts involved. Though the amount are small, this tactic can be very costly to the company involved. For example, a programmer from a U.S. bank gathered nearly $132,000 in various fictitious accounts. This individual, as with most others, was discovered by chance. In a publicity contest, this bank offered a prize to the account holder with the strangest name. One of the fictitious accounts was chosen as a winner. When the "owner" never claimed the prize, the bank investigated and discovered the crime (San Segundo, 1985, p. 47).

These cases illustrate the diverse nature of computer crime in general. The most important thing to note after reading these cases is that each case involving computer crime is necessarily different. There is no easy way to classify crimes into various categories. Since each company has an accounting system modified to serve its individual needs, the perpetration of any crime involving that system will involve unique aspects to manipulate that specific system and to get around the specific controls present. Therefore, no two computer crimes will be identical.

Criminal Characteristics

While it is difficult to find common characteristics concerning the crimes, themselves, it is possible to identify some common characteristics of the computer criminals. The more "traditional" criminals (i.e. thieves, murderers, etc.) tend to have rather shady backgrounds cluttered with drug abuse, child abuse, and no formal education. Computer criminals, on the other hand tend to possess quite admirable backgrounds, as the following common traits illustrate.

Well Educated

One of the major characteristics possessed by most computer criminals is a good education. Most have, at a minimum, a high school education, with the majority also achieving a college degree. This trait is logical, given the nature of computer work. As the computer age rolls along, more and more education in the computer area is required to obtain a position working with computers. Therefore, in order for these criminals to obtain jobs which place them in a position to perpetrate such crimes, they must be well educated.

Intelligent

A second characteristic common to most computer criminals is intelligence. These types of criminals must possess a high degree of intelligence to plan the crime and cover their tracks. Often, very elaborate controls are in place governing the computer system. The criminal, then, must be able to understand the existing controls and visualize a way around them. Moreover, the criminal must then be

able to conceal the crime and leave no way for the authorities to trace it back to the perpetrator.

Creative

Creativity is a characteristic which naturally follows intelligence. Since each company usually has a system modified to their unique needs, the method of committing each crime will differ. Since the criminal will be facing a new challenge and conditions never encountered before, creativity is a prerequisite to circumventing the controls. The criminal will have to be able to visualize unique and untested methods to perpetrate their plan.

Noncriminal Background

A third trait typical to most computer criminals is a "clean" background. It is quite common for individuals convicted of computer crime to have no prior criminal record. Again, to earn a position which will allow the criminals to pull off these types of crimes, the individual must have a near spotless record, and earn the trust of their superiors. People who have a history of criminal activity will have a harder time earning the trust of their managers and will be less likely to be placed n sensitive positions allowing them the opportunity to execute computer crimes.

Highly Motivated

Another common characteristic exhibited by most computer criminals is a high level of motivation. To this point, this thesis may have given the impression that computer crime is simple perpetrate. On the contrary, these crimes are quite

difficult and time consuming. It requires a large amount of planning and hard work to pull it off. For this reason, the computer criminals must possess a high level of motivation to propel them to undertake such a painstaking task. People who are lazy or who lose interest in what they are doing would never be able to pull off such elaborate crimes such as those previously illustrated. Additionally, computer criminals often engage in such activity for the mere challenge of trying to "beat the computer", which, again, involves a certain degree of motivation.

Patient

Closely related to high motivation, patience is another trait found in most criminals of this type. Many times, computer crime involves mere trial and error. A previously mentioned, most systems do have a certain degree of control devices programmed into them, such as access codes and passwords. The computer criminal, then, must have the patience and perseverance to try a different path if the one they are trying leads to a dead end. This patience allows them to remain calm, not get frustrated, and pursue another path, a process which may encompass days or weeks.

Ethical

Perhaps the most surprising characteristic of computer criminals is that nearly all of them consider themselves to be very ethical. Most of these people wouldn't ever think of stealing anything at gunpoint or of physically hurting anyone else, and, more often than not, view themselves as having high moral standards.

They engage in this type of activity because they don't see it as hurting anyone. The computer is a very impersonal device, and as such, "moral" people don't see anything wrong with trying to manipulate the system for their benefit, especially after seeing billions of dollars being transferred from one computer to another. Again, it comes back to the challenge of beating the computer and the glamour associated with this type of crime. However, as illustrated in the international spy ring case, often times these crimes can come very close to hurting, even killing real people, whether intentional or not.

The most ironic feature about this portrait of the computer criminal we have just painted is that these are all qualities employers look for in a "good employee", and they are the qualities people are told to emphasize when interviewing for a job. Having been a Presidential Scholar for four years, I can also say that these are the very same traits exhibited by all the Presidential Scholars, thus making the university's best students prime candidates as computer criminals.

Additionally, many of the people convicted of computer crime later end up working as consultants to companies, offering advice on the company's controls and how to tighten security. Ian Murphy, one of the first people to be convicted of computer crime, was caught as part of a ring of eight hackers. This ring ran up nearly $212,000 in fraudulent telephone calls and another $200,000 in hardware ordered using stolen credit card numbers and false mailing addresses. Murphy now does consulting work for companies, teaching them how to detect computer crime.

Murphy charges $800 per day, and some of his major clients include Monsanto, Peat Marwick, United Airlines, and General Foods (Kneale, 1987, p. A1).

The above characterization the common computer criminal is very accurate. However, as computer crimes are becoming more frequent and more publicized, a second group of computer criminals is emerging that differs from the above illustration in two important areas. These new criminals are neither highly intelligent nor creative. These criminals simply rely on the previous work of other criminals and use old techniques to tackle new problems. This was exactly the method used by the intruder in the Lawrence Berkeley Lab in California. As Clifford Stoll commented, "He showed neither brilliance nor creativity. He was patient, but he used old methods of illegal access," (Stoll, 1988, p. 485). In fact, an underworld computer network now exists for computer criminals. This network contains "community billboards" with access codes on it which have been placed there by other hackers for the benefit of the rest of the underworld(Kneale, 1987, p. A22).

Preventive Controls

Having examined what types of crime are committed and who commits them, we can now look at some of the various controls that can be used to deter this type of activity. A good internal control system to ensure safeguarding of assets and records and to assure enterprise goals are being met is essential in any business, whether they have a computerized accounting system or not. But such controls become much more important in a computerized environment, where the susceptibility to misuse is increased.

Separation of Related Functions

The separation of duties is one of the most important controls needed. This ensures that no one person should be responsible both for the custody of an asset and also for the recordkeeping regarding that asset. This control is especially important in a computerized system, where misappropriations are concealed much easier. This separation of duties will then serve as a check and balance system, since two or more people are responsible for the various areas concerning a given asset. If one person tries to misappropriate the asset, the other person(s) responsible for it should detect the error.

Limited Access to Computer/Records

A second important internal control in a computerized environment is limited access to the computer and to computer records. Personnel who have no authority to use the computer should not be allowed access to it at all. Those

employees who do have authority to use the system should not be able to access information related to their specific tasks. For example, if responsibility for accounts receivable and accounts payable are given to two separate people, controls should be in place so that the receivables person cannot access payable information and vice versa.

Moreover, people who have been terminated should be completely restricted any access to the computer, even if they were previously authorized to use it. Many times a disgruntled employee who has been let go will, in a fit of rage, sabotage the computer or the records if allowed continued access in the two weeks after notice of termination. This activity can be devastating to a company, therefore these individuals should have completely restricted access.

Enforcement of Vacations

A simple, yet extremely effective control that can detect fraudulent activity is the enforcement of mandatory one or two week vacations. This technique is especially effective in detecting crimes such as the previously mentioned lapping of accounts receivable, where the perpetrator needs to be present on a daily basis to keep the scam going. By enforcing the vacation rule, new people will fill in and the lapping scheme will cease. This will allow any improprieties to be brought to the surface, since their will be a gap in the accounts between the last account credited by the lapper and the first correct account credited by the interim person. The accounts in this gap will never be credited, and when these customers receive their

billing statements, they will complain, revealing the crime.

Keep Employees Happy

Finally, and most importantly, management should try to keep the employees satisfied. This does not mean giving in to the workers' every wish, but merely keeping the labor-management relations on an amiable basis. If management gives the workers reason to "get even", they will start looking for ways such as computer fraud to get their revenge. If the workers are content and feel that they are part of the company team, they will be less likely to perpetrate such crimes for fear that they are hurting the company.

It is important here to note that the best these controls can do is *reduce the likelihood* of the occurrence of such crimes. Given the interdependency between the employees in any system, no control can provide complete assurance that such crimes will be totally eliminated. Computer crime is a very difficult activity to detect, and an even tougher activity to prevent, since mere detection does not guarantee prevention. Returning to the LBL case, after the intruder was apprehended, LBL tightened the controls in its system, but even with the modifications, a summer student testing the new controls still found many holes in the system.

The sad fact of the matter is, however, that most of the crimes that are detected are discovered, not by elaborate and expensive controls, but rather by mere chance. This point is graphically illustrated by the cases illustrated earlier,

where not one of the crimes was detected by a control procedure designed to catch these acts. More often that not it is a disgruntled employee or an enraged customer who reveals the crime. Indeed, this is a difficult activity to detect, even when the perpetrator *expects* to be caught. The intruder in the LBL case, for example, thought others knew of his intrusions. As Clifford Stoll stated, "From the intruder's viewpoint, almost everyone but LBL detected his activity. In reality, almost nobody except LBL detected him," (Stoll, 1988, p. 486).

Responsibility for Detection

To this point, this paper has focused on computer crime from the vantage point of the company, itself. As a final angle on this subject, this paper will now examine the role an independent auditor plays in discovering fraudulent uses of computerized accounting systems and how the responsibility for detection of these act is divided between the company and the auditor.

In addition to the company, itself, the only other person in any position to detect such activity is the independent auditor. An auditor may be engaged to either express an opinion on the company's financial statements or, more specifically, to express an opinion on the company's internal control system.

Primary guidance on how an auditor should conduct an audit and the degree of responsibility she takes comes from the American Institute of Certified Public Accountants' (AICPA) Statements on Auditing Standards. These standards outline ten generally accepted procedures to be followed in every audit, but they don't address computer crime, per say. Under these standards, an auditor must obtain an adequate understanding of the computer system and the internal controls thereon to assess the risk that irregularities may occur. From this assessed risk, the auditor must obtain evidence to provide reasonable, not absolute, assurance that these types of activities are discovered.

The Statements on Auditing Standards do prescribe different procedures to be applied when auditing a computerized system, but the level of responsibility

remains the same - to provide reasonable assurance. This gives rise to what has been called the "expectation gap" between the actual responsibility of an independent auditor and the level of responsibility expected by their client and the general public. Neither management nor the auditor wants to accept the responsibility for detecting computer fraud.

Additionally, the AICPA's auditing standards require that the audit be performed by persons having adequate training and proficiency as an auditor. While this requirement does specify that this encompasses education *and* experience, it does not specifically address what constitutes this level of proficiency, especially in terms of computer knowledge. It is this type of vaguety which allowed the Wolfson, Weiner firm to audit Equity Funding and prevented that fraud from being discovered. A specified level of adequate proficiency in computers for auditors is another issue which must be addressed in the years to come.

The question then arises, "Who should bear the responsibility for curtailing this problem?" The answer can only fall on four individuals: the maker of the software, the company, the independent auditor, or the police responsible for catching the criminals. Clifford Stoll, the astronomer who exposed the spy ring, has noted serious deficiencies in software sold by vendors. The vendors often distribute weak software to the companies. These programs have few controls installed, and many times have backdoor entryways and default codes left in them

from the development stages. Moreover the installers of the systems show little concern for security (Stoll, 1988, p. 493). However, since each buyer will be usually modify the programs to their individual needs, it is difficult for the vendor to provide controls to meet every need, and holding them responsible for this problem seems somewhat unfair.

As for the individual companies, they buy the computer systems for their capability, not for their security. All too often, the systems managers don't see a need for such controls until after they have been victimized. Ian Murphy, the hacker/consultant, blames corporate stupidity and laziness for the problems with computer crime. But an important point to remember her is that a company should utilize controls only if the expected benefit of these controls will outweigh the costs involved. Since many of the controls are very expensive, it is often impracticable for companies, especially small companies, to utilize them. Therefore, it is hard to hold the companies responsible, either. Ivars Peterson states, "The only thing you can do is make unauthorized access more difficult. You can never make it impossible. It becomes a question of how much a company is willing to pay - in inconvenience and in dollars," (Peterson, 1983, p. 294).

As for the auditors, given their limited involvement with their clients, it seems inappropriate to hold them responsible for detecting such crimes beyond the "reasonable assurance level". As these types of crimes are inherently difficult to detect, especially when it is a joint effort, the independent auditor is not in any

position to provide absolute assurance of detection. A possible solution might be to require accounting firms to hire computer specialists and assign this person to all engagements involving computerized systems. This might increase the level of assurance provided by audits.

The police offer a final party who may be able to help deter computer criminals. As it stands right now, though, the police are not capable of handling these cases. These crimes are usually handled by the local authorities, who lack sufficient training in the computer area to adequately handle the case. Also, the cases typically take too long to prosecute for effective deterrence. Kenneth Rosenblatt, a researcher in deterrence of these crimes, concludes that the police can play a more effective role in alleviating this problem. He contends that to deter his activity, the potential criminals must be convinced that they *will* be apprehended, and that the punishment will be very unforgiving. Additionally, Rosenblatt argues that the enforcement of these crimes should be taken out of the hands of the local police and placed in the hands of state and federal authorities, who can better train individuals in this area (Rosenblatt, 1990).

It would seem, then, that no one party is in a very good position to step to the fore and accept responsibility for alleviating this problem. Perhaps increased efforts on all three fronts will help the problem. This is an issue which will be receiving much attention in the next few years, and perhaps new litigation will more clearly define the roles to be played by each of the parties.

Conclusion

Computer crime is a difficult problem to address. Companies are very reluctant to talk about it, each crime is unique and hard to detect, and no one wants to take responsibility for detecting or preventing such crimes. Moreover, the distinguishing traits of the average computer criminal are also the desirable characteristics of quality employees, and no control is sure-fire.

Given the difficult nature of the problem, I can offer no hard and fast recommendations or findings to rectify this particular situation. As mentioned earlier, someone is going to have to step forward and take a leading role in deterring this activity. I think the next few years will bring increased attention to this problem on all fronts. Companies will beef up controls, the AICPA may establish new guidelines in this area for auditors, computer vendors may provide more controls in their packages, and police will attempt to establish more rigid enforcement. Whatever the solutions that are implemented, they will have to be flexible enough to change with the changing computer technology.

Yet, merely increasing the efforts will not guarantee that the problem will go away. As illustrated in the preceding pages, there is no way of providing absolute assurance of eliminating computer crimes altogether. Perhaps the best way for a company to feel safe about their system is to devote strong effort to hiring trustworthy employees, establish a trusting relationship with them, and keep them content. As for the employees,themselves, they need to realize that by working

with computers, they are in a sensitive position. As such, they need to have a stronger ethic regarding their behavior, and they should accept a greater responsibility to the company for which they work. Only through a combined effort in these last two areas can society be certain that computer crime will cease to be the problem it is today.

Sources Cited and Consulted

Albanese, J. S. (1988). Tomorrow's thieves. The Futurist, 22(5), pp. 24-28.

American Institute of Certified Public Accountants. (1990). Statements on Auditing Standards. Chicago: Commerce Clearing House, Inc.

Andrews, F., Epstein, M. J., and Seidler, L. J. (1977). The Equity Funding Papers. New York: John Wiley and Sons.

Boch, G. (1988). The chairman and his board. Time, May 30, #22, p. 45.

Dirks, R. L. and Gross, L. (1974). The great Wall Street scandal. New York: McGraw-Hill Book Co.

Dallos, E. and Soble, R. L. (1975). The impossible dream. New York: G. P. Putnam's Sons.

Ferrell, K. (1990). If you want to see the typical computer criminal, just look in the mirror. Compute, 12(5), p. 99.

Johnson, D. W. (1984). Computer ethics: a guide for a new age. Elgin, Illinois: The Brethren Press.

Kneale, D. (1987). It takes a hacker to catch a hacker, as well as a thief. The Wall Street Journal, November 3, p. A1, A22.

Moscove, S. and Simkin, M. (1987). Accounting information systems. New York: John Wiley and Sons.

Peterson, I. (1983). Computer hacking and security costs. Science News, November 5, #124, p. 294.

Rosenblatt, K. (1990). Deterring computer crime. Technology Review, 93(2), pp. 34-40.

San Segundo, G. (1985). The cost of computer crime. World Press Review, 35(1), p. 47.

Shapiro, S. (1984). Wayward capitalists. New Haven: Yale University Press.

Stoll, C. (1988). Stalking the wiley hacker. Communications of the ACM, 31(5), p. 484-497.

Stoll, C. (1989). The cuckoo's egg: tracking a spy through the maze of computer espionage. New York: Doubleday.

Wagner, C. R. (1979). The C.P.A. and computer fraud. Lexington, Massachusetts: Lexington Books.