COMPUTER CRIME
CAREER OF THE FUTURE?

Jay Becker
National Center for Computer Crime Data

"The odds are one in twenty-two thousand that a computer criminal will go to jail."

In a nutshell, there are several good reasons why you might consider a career in computer crime. First of all, no one will ever know if you commit one. Second, no one will ever tell if you do. Third, no one will ever punish you. Fourth, you really don't have to know an awful lot about computers to commit this crime. Fifth, the opportunities for advancement are phenomenal. And, finally, there's no time like the present.

It doesn't take an awful lot of imagination to envision the growth of computer crime. Everywhere, computer use is increasing. With personal computing becoming more and more accessible, one can only assume that the number of computer users and uses is likely to grow, with even greater speed in the next decade than it has in the last.

Against this background, I want to consider the appeal of computer crime to the would-be criminal. My purpose is not foster this crime, but to alert its potential victims. And if you're a businessman or woman, if you invest in any business, if you buy the products or services of any business, or if you pay taxes, victim means you.

The tongue-in-cheek recommendations that I make are a reflection of the alarm that I feel based on my conversations and readings. They cry out for action. Perhaps you will help

Reprinted with permission from the author as printed in Computer Careers Magazine, October, 1980.

No One Will Ever Know

The statistic that computer crime experts are wont to throw around is that one percent of all the computer crimes ever committed are detected. (You might wonder, if you're of a logical bent, how you calculate a percentage of a number you don't know. That's a really heavy logical problem.) But victimization studies in related areas, and fairly wide guestimates, have been used to at least give us a starting point for discussion. Now, why is that so? There are technical reasons. Consider the setting. A computer may well process 1,000,000 orders or disburse hundreds of thousands of checks each year. The programming may run into hundreds and thousands of instructions and computer operations. It's hard to find a little part of the program that has been insinuated into a system to help commit a crime. A programmer may even instruct the computer to erase the larcenous instruction after the crime has been committed. These technical problems are just the beginning. The main reasons that computer crime is not detected are either economy or psychological. People setting up computer systems often have not spent the money necessary to prevent or detect computer crimes. The software and the hardware are such that just about any crime that you can imagine, someone else can imagine an expensive, computer system to prevent or detect it. So any system that is victimized is not victimized except because the money was not spent to prevent that sort of victimization.

Now, why is the money not spent? Part of the reason is lack of foresight. Many people who buy computer systems don't give much thought to some criminal ripping the system off ten years down the line. They are usually very concerned with improving over a manual operation or a smaller computer system, because their present system is not adequate to meet pressing needs like getting the damn paychecks out on time, like getting the inventory up to date. All too often the last thing a business wants to worry about is some hypothetical problem from some undiscovered criminal somewhere in the distant future. That's bad enough

But there's also the psychology of computers which fascinates me. Call it the computers which fascinates me. Call it the computer mystique. A Deputy U.S. Attorney General made a very cogent observation about the psychological effect of computers. He said, "Consider the businessman who would never leave his checkbook lying on top of his desk, who requires a double signature on each corporate check, who would never discharge a sensitive employee without changing the lock on the door and the combination on the office safe, and who would be aghast if his banker informed him that, as an economy measure, he was no longer returning cancelled checks. This same businessman will purchase a multi-million dollar computer system from an energetic salesman without provisions for an audit as basic as a cancelled check. He will place this computer terminal on top of his desk, unattended, and will use a programmer to design his entire system, and will discharge this programmer without making the most rudimentary changes in his computer's security system.

Law and ethics present additional problems which keep the detection of computer crime from being as great as it might be. Donn Parker, who's probably the expert in computer crime, has done some research and given out some questionnaires asking people about their point of view about the ethics involved in different computing situations. Consider trying to break into a system to use it for your own benefit, or trying to use a program that someone else developed. Parker asked different people whether those acts were criminal, whether they were unethical, and whether they were things that the people who were answering the surveys had themselves done. And he took these surveys in the computer industry, in the EDP auditing industry, and on the management level of the corporate structure, and he found enormous variation in people's opinions as to what was criminal and what was wrong and what was something that was perfectly proper for them to do.

The last point which supports the estimate of one percent for detection is the ways in which computer crimes were detected. Most of them read like Alan Arkin or Peter Sellers mysteries where, you know, the detective just kind of trips and hits his head on something or other and something bounces off and ah hah, the crime is solved. For instance, one fellow had a fairly sophisticated round-down system going. If there's a little fraction of a cent in your bank account, usually it's fairly distributed over all the accounts. Instead, the criminal set up a system where all these little fractions would be credited to his account and over the course of time he was able to get fairly rich. He named his account Zwana and it was last in a series of customer accounts. One day the companys' PR section said, "Let's celebrate something or other and thank the first and the last person in our account system." So they looked up Mr. Attleburt and sent him a letter saying, "We want to congratulate you on being our first account." And then they tried to find Mr. Zwana and the criminal's days were numbered and he ultimately got caught. But, you can't rely on too many PR agents if you're trying to set up a security system. Since we don't find people through auditing procedures or through computer-generated diagnostics when they try to commit crimes, as often as we'd like, but through happenstances, we infer that not many of them are really caught.

No One Will Tell

You've committed the crime and lo and behold, it's been detected. We estimate that no more than 15 percent of the people detected are ever reported to the police. What's that? Three out of 20. Now why you would want to ask, I hope, don't the other 17 out of 20 get reported? Part of the reason is more mythology. People who have a stake in the computer myth are loathe to facilitate its being dissolved. If you have a bank and you've advertised "Our computer will safeguard your money. Our computer never makes mistakes," the worst thing in the world for you is if hundreds of people start thinking, "Hey. Computers get ripped off all the time. I don't want my money guarded by a computer. Maybe these computers aren't as special as all the advertisements and news articles and special features have told us over the last two decades."

The average loss in a computer crime case is about $450,000, those 85 percent who aren't reporting cases are absorbing enormous losses. As I said earlier, they're not really absorbing the losses. Ultimately, we are. And when losses like that, whether they're related to the computer or not, are not made public because people think the PR is really bad, well, then we suffer. The danger is real. A fellow got caught committing a crime and his employers threatened to fire him. He turned the tables on them. "Who do you think you are, threatening me? I'm gonna threaten you. If you fire me and don't give me an excellent recommendation," he said, "(so I can get a better computer job), I'm gonna let the world know what a lousy system you have. Just think what that's gonna do to your PR and what that's gonna do to your stockholders." And the company buckled under. They said "okay" and they wrote him a letter saying, "This is a wonderful employee. He's trustworthy, loyal, helpful, friendly" blah, blah, and he got another job in another computer company and he stole again. This is the prosecutor's problem and the criminal's delight.

No One Will Punish You

Of those who come before the tender mercies of prosecution and the court, only one out of every 33 people actually goes to jail. And, if you want some quick mathematics, one-one hundreth times three twentieths times one-thirty third means the odds are one in twenty two thousand that a computer criminal will go to jail. Again, we ask why. In law enforcement minds, the computer mystique is often alive and well. Usually the investigator is not equipped. He or she has gone through college, but most likely has had very little to do with computers (though, of course, that's changing). Someone comes in and confronts the investigator with a stack of computer printouts and says, "I think I've been robbed." The stack is kind of a mystery. So a lot of people are going to be loathe to involve themselves in something they know absolutely nothing about. Others will try, but they won't be able to do as good a job as someone who knows about computers.

In addition to these problems of just understanding a computer on the level of investigation, if the case goes to court, you have to deal with antidiluvian laws in some jurisdictions. I got a call recently from a prosecutor in a mid-Western state who told me that students at the university had kind of done extra-mural work in the field of computer sciences. They bought a Heathkit setup and made a computer terminal, used it to access the university's computer, and began to use the computer to do all of their homework problems that involved computations. They developed their own account so that no one was victimized but the university. They got a substantial amount of time. The prosecutor called me because none of the statutes in his state covered the theft of computer time. To remedy problems like this, the state of Florida passed a bill specifically addressed to

computer crimes. Congress is considering a similar bill, as are California, Maryland, and Illinois.

The Chances For Advancement Are Great!!

Jerry Neil Schneider, one of the more famous computer criminals, is I think,a real inspiration for anyone seeking employment in the field. At the tender age of 19, Schneider developed a system to swindle the Pacific Telephone company. He had it working so that he could get the telephone company system to deliver parts to him and he had a truck all painted up and at odd hours in the night he would go and pick up these parts that the telephone company had delivered to him for free because he had gotten into their computer system. Over five years he stole approximately $250,000. Finally he was detected, (not through any investigation by law enforcement), but because one of his employees got mad that he wasn't getting enough pay. After detection, Jerry's career took off. The best thing in the world that could happen for him was to be detected. National publicity visited him in his crime. He settled a civil suit growing out of the incident by agreeing to pay the phone company a grand total of less than $9,000, leaving, one assumes, a profit of $241,000. He did serve 40 days in County jail. But that's the smallest part of it. Trading on his fame as a computer criminal, he went into business as a consultant to people who did not want to be ripped off by computer criminals. Rumor has it (and this has never been confirmed or denied that I know), included among his clients was Pacific Telephone Company, which was still rather curious exactly how it was that he accomplishes some of his feats. Certainly, thanks to the publicity of his conviction, he, like perhaps ex-president Nixon and others, showed that sometimes getting caught is the most economical thing a criminal can do.

You Needn't Be A Genius

You may wonder what it takes to commit these crimes. I mean, certainly Jerry Schneider was a pretty clever guy. He was able to do what very few people could do with the phone company. Many cases do involve that expertise. But not all. The slow, lame, and blind can also consider computer crime. One fellow operated a check printing output station of a computer and among the other payroll checks that it printed was his own. In case a mistake is made by the printer--it prints "Lithelstick" instead of "Jay Becker"--there's a Repeat button and one's supposed to tear up the inappropriate check and hope that the computer does it right the second time. Well, this very sophisticated thinker figured out that if he pressed the Repeat button when his own check came up, he could make a fortune. So, he pressed the Repeat button a whole bunch of times and came out with a large number of checks. As I say, you don't have to be a genius. This fellow proved that he certainly wasn't because he took all the checks that he had printed and brought them to the same teller at the same bank at the same time, and she being above the level of Mongoloid, decided that there must be something wrong because he got paid 18 times for the same time period. He was subsequently arrested and taught to be more discrete. Another of my favorites that doesn't involve any knowledge of computers or computer systems at all is a very simple thing of opening a checking account, getting a book of deposit slips, and each is encoded in a machine-readable form "Credit this deposit to the account of Joe Criminal." Joe goes to a printer and gets a whole bunch of blank deposit slips and has printed in machine-readable but invisible magnetic stuff "Credit this deposit to the account of Joe Criminal." Joe then goes to the bank, goes to the deposit slip holder where there are a bunch of blank deposit slips, takes them out, puts his deposit slips in, and then whenever someone writes out a check and makes a deposit to their own account, Joe Criminal comes out that much ahead. This scheme has been used in several places. This scam is why there are not longer deposit slips dispensers available to the public in banks.

There's No Time Like The Present

With all these great statistics and opportunities and lack of entry requirements, one might think, "Gee, why don't I finish my degree, hit my parents up for $20,000, and go around the world for a year and a half, and after contacting more or less of the desirable social diseases, settle down to a life of leisure in computer crime." Well, I wouldn't wait if I were you because the various segments of society which are interested in computer crime are acting and trying to right the balance. The National Center for Computer Crime Data is but one little part of the picture. I send people documents from computer crime cases that seem analogous to their own or refer them to someone local who can be of assistance, either a prosecutor or an investigator who has experience in computer crime cases, or some kind of other expert in computing or account
work--in the old chavinist days we'd call it an old boy network; now we call it an old person network--of people willing to be of assistance to other people investigating or prosecuting computer crime. More and more prosecutors and investigators are learning how to do this. I've either attended or spoken at training sessions for prosecutors and investigators that the FBI has sponsored in Quantico, Va., that Batelle Research Institute had up in Seattle, that the Florida Institute of Law Enforcement has had in St. Petersburg. Thus, throughout the country, law enforcement is being educated in computers and is developing the expertise to deal with problems associated with them. And, as I say, legislation is being considered in the crime in several states. I'm sure that the legislature of the state that I told you about had its problem is going to be receiving bills from legislators who have been goosed by the newspaper saying "How come our state can't prosecute computer crimes?" So, throughout the nation, my expectation is that more and more laws are going to be passed directly relating to computer crime. And other interested groups are mobilizing. The computer industry, through the Association For Computing Machinery and the American Federation of Information Processing Societies, accounting groups, the American Society For Industrial Security all see the problem, and through various study groups and projects are trying to deal with it.

Let me leave you with this concluding question: If for the would-be computer criminal the time to act is now, when must the rest of us act?

Jay Becker is a Deputy District Attorney in Los Angeles and the Director of the National Center For Computer Crime Data. Becker has lectured extensively on the subject of computer crime. He is editor of the computer crime special issue of the Computer/Law Journal, the author of "Investigation Of Computer Crime," and a frequent writer on the topic. Other of his writings include editorials in the Los Angeles Times and San Diego Union on computer crime, reviews in the Washington Post and Security Management, and other articles in Security World, Crime and Delinquency, The Prosecutor's Brief, and Law Office Economics and Management.

Mr. Becker is Chairman of the National District Attorneys Association Committee on Information Systems, a member of the American Society for Industrial Security, and its subcommittee on computer crime, and a member of the ACM, ABA Section on Science and Technology, and Los Angeles County Bar Law and Technology Committee.

S240, approved Nov. 6, would make it a crime to use or attempt to use a computer with the intent to execute a fraudulent scheme, obtain property by false pretenses, embezzle, steal or convert another's property.

Possible penalties would include a fine of not more than two times the amount of gain or $50,000, whichever is higher, five years in prison, or both.

The bill also would make it a crime to intentionally damage a computer. The penalty for this offense would be a fine of up to $50,000, imprisonment for not more than five years, or both.

The federal government would be given authority to prosecute either crime if the computer involved is owned or operated by the United States or a federally-insured financial institution. The government also could prosecute if the computer were operated in interstate commerce or used "a facility of interstate commerce."

The bill would not require that the illicit computer penetration be accomplished by interstate facilities--such as telephone lines--to consider the act a federal offense.

The federal government would not have to prosecute a case if a state also had jurisdiction over the matter.