Computer crime 13829

Laws must be passed to address the increase in the number and types of computer crimes. Over the last twenty years, a technological revolution has occurred as computers are now an essential element of today’s society. Large computers are used to track reservations for the airline industry, process billions of dollars for banks, manufacture products for industry, and conduct major transactions for businesses because more and more people now have computers at home and at the office. People commit computer crimes because of society’s declining ethical standards more than any economic need. According to experts, gender is the only bias. The profile of today’s non-professional thieves crosses all races, age groups and economic strata. Computer criminals tend to be relatively honest and in a position of trust: few would do anything to harm another human, and most do not consider their crime to be truly dishonest. Most are males: women have tended to be accomplices, though of late they are becoming more aggressive. Computer Criminals tend to usually be “ between the ages of 14-30, they are usually bright, eager, highly motivated, adventuresome, and willing to accept technical challenges.”(Shannon, 16: 2) “ It is tempting to liken computer criminals to other criminals, ascribing characteristics somehow different from ‘ normal’ individuals, but that is not the case.”(Sharp, 18: 3) It is believed that the computer criminal “ often marches to the same drum as the potential victim but follows and unanticipated path.”(Blumenthal, 1: 2) There is no actual profile of a computer criminal because they range from young teens to elders, from black to white, from short to tall. Definitions of computer crime has changed over the years as the users and misusers of computers have expanded into new areas. “ When computers were first introduced into businesses, computer crime was defined simply as a form of white-collar crime committed inside a computer system.”(2600: Summer 92, p. 13) Some new terms have been added to the computer criminal vocabulary. “ Trojan Horse is a hidden code put into a computer program. Logic bombs are implanted so that the perpetrator doesn’t have to physically present himself or herself.” (Phrack 12, p. 43) Another form of a hidden code is “ salamis.” It came from the big salami loaves sold in delis years ago. Often people would take small portions of bites that were taken out of them and then they were secretly returned to the shelves in the hopes that no one would notice them missing.(Phrack 12, p. 44) Congress has been reacting to the outbreak of computer crimes. “ The U. S. House of Judiciary Committee approved a bipartisan computer crime bill that was expanded to make it a federal crime to hack into credit and other data bases protected by federal privacy statutes.”(Markoff, B 13: 1) This bill is generally creating several categories of federal misdemeanor felonies for unauthorized access to computers to obtain money, goods or services or classified information. This also applies to computers used by the federal government or used in interstate of foreign commerce which would cover any system accessed by interstate telecommunication systems. “ Computer crime often requires more sophistications than people realize it.”(Sullivan, 40: 4) Many U. S. businesses have ended up in bankruptcy court unaware that they have been victimized by disgruntled employees. American businesses wishes that the computer security nightmare would vanish like a fairy tale. Information processing has grown into a gigantic industry. “ It accounted for $33 billion in services in 1983, and in 1988 it was accounted to be $88 billion.” (Blumenthal, B 1: 2) All this information is vulnerable to greedy employees, nosy-teenagers and general carelessness, yet no one knows whether the sea of computer crimes is “ only as big as the Gulf of Mexico or as huge as the North Atlantic.” (Blumenthal, B 1: 2) Vulnerability is likely to increase in the future. And by the turn of the century, “ nearly all of the software to run computers will be bought from vendors rather than developed in houses, standardized software will make theft easier.” (Carley, A 1: 1) A two-year secret service investigation code-named Operation Sun-Devil, targeted companies all over the United States and led to numerous seizures. Critics of Operation Sun-Devil claim that the Secret Service and the FBI, which have almost a similar operation, have conducted unreasonable search and seizures, they disrupted the lives and livelihoods of many people, and generally conducted themselves in an unconstitutional manner. “ My whole life changed because of that operation. They charged me and I had to take them to court. I have to thank 2600 and Emmanuel Goldstein for publishing my story. I owe a lot to the fellow hackers and fellow hackers and the Electronic Frontier Foundation for coming up with the blunt of the legal fees so we could fight for our rights.” (Interview with Steve Jackson, fellow hacker, who was charged in operation Sun Devil) The case of Steve Jackson Games vs. Secret Service has yet to come to a verdict yet but should very soon. The secret service seized all of Steve Jackson’s computer materials which he made a living on. They charged that he made games that published information on how to commit computer crimes. He was being charged with running a underground hack system. “ I told them it was only a game and that I was angry and that was the way that I tell a story. I never thought Hacker [Steve Jackson’s game] would cause such a problem. My biggest problem was that they seized the BBS (Bulletin Board System) and because of that I had to make drastic cuts, so we laid of eight people out of 18. If the

Secret Service had just come with a subpoena we could have showed or copied every file in the building for them."(Steve Jackson Interview) Computer professionals are grappling not only with issues of free speech and civil liberties, but also with how to educate the public and the media to the difference between on-line computer experimenters. They also point out that, while the computer networks and the results are a new kind of crime, they are protected by the same laws and freedom of any real world domain. " A 14-year old boy connects his home computer to a television line, and taps into the computer at his neighborhood bank and regularly transfers money into his personnel account."(2600: Spring 93, p. 19) On paper and on screens a popular new mythology is growing quickly in which computer criminals are the ' Butch Cassidys' of the electronic age. " These true tales of computer capers are far from being futuristic fantasies."(2600: Spring 93: p. 19) They are inspired by scores of real life cases. Computer crimes are not just crimes against the computer, but it is also against the theft of money, information, software, benefits and welfare and many more. " With the average damage from a computer crime amounting to about $. 5 million, sophisticated computer crimes can rock the industry."(Phrack 25, p. 6) Computer crimes can take on many forms. Swindling or stealing of money is one of the most common computer crime. An example of this kind of crime is the Well Fargo Bank that discovered an employee was using the banks computer to embezzle $21. 3 million, it is the largest U. S. electronic bank fraud on record. (Phrack 23, p. 46) Credit Card scams are also a type of computer crime. This is one that fears many people and for good reasons. A fellow computer hacker that goes by the handle of Raven is someone who uses his computer to access credit data bases. In a talk that I had with him he tried to explain what he did and how he did it. He is a very intelligent person because he gained illegal access to a credit data base and obtained the credit history of local residents. He then allegedly uses the residents names and credit information to apply for 24 Mastercards and Visa cards. He used the cards to issue himself at least 40, 000 in cash from a number of automatic teller machines. He was caught once but was only withdrawing $200 and in was a minor larceny and they couldn't prove that he was the one who did the other ones so he was put on probation. " I was 17 and I needed money and the people in the underground taught me many things. I would not go back and not do what I did but I would try not to get caught next time. I am the leader of HTH (High Tech Hoods) and we are currently devising other ways to make money. If it weren't for my computer my life would be nothing like it is today."(Interview w/Raven) " Finally, one of the thefts involving the computer is the theft of computer time. Most of us don't realize this as a crime, but the congress consider this as a crime."(Ball, V85) Everyday people are urged to use the computer but sometimes the use becomes excessive or improper or both. For example, at most colleges computer time is thought of as free-good students and faculty often computerizes mailing lists for their churches or fraternity organizations which might be written off as good public relations. But, use of the computers for private consulting projects without payment of the university is clearly improper. In business it is the similar. Management often looks the other way when employees play computer games or generate a Snoopy calendar. But, if this becomes excessive the employees is stealing work time. And computers can only process only so many tasks at once. Although considered less severe than other computer crimes such activities can represent a major business loss. “ While most attention is currently being given to the criminal aspects of computer abuses, it is likely that civil action will have an equally important effect on long term security problems.”(Alexander, V119) The issue of computer crimes draw attention to the civil or liability aspects in computing environments. In the future there may tend to be more individual and class action suits. CONCLUSION Computer crimes are fast and growing because the evolution of technology is fast, but the evolution of law is slow. While a variety of states have passed legislation relating to computer crime, the situation is a national problem that requires a national solution. Controls can be instituted within industries to prevent such crimes. Protection measures such as hardware identification, access controls software and disconnecting critical bank applications should be devised. However, computers don’t commit crimes; people do. The perpetrator’s best advantage is ignorance on the part of those protecting the system. Proper internal controls reduce the opportunity for fraud.

BIBLIOGRAPHY Alexander, Charles, “ Crackdown on Computer Capers,” Time, Feb. 8, 1982, V119. Ball, Leslie D., “ Computer Crime,” Technology Review, April 1982, V85. Blumenthal, R. “ Going Undercover in the Computer Underworld”. New York Times, Jan. 26, 1993, B, 1: 2. Carley, W. “ As Computers Flip, People Lose Grip in Saga of Sabatoge at Printing Firm”. Wall Street Journal, Aug. 27, 1992, A, 1: 1. Carley, W. “ In-House Hackers: Rigging Computers for Fraud or Malice Is Often an Inside Job”. Wall Street Journal, Aug 27, 1992, A, 7: 5. Markoff, J. “ Hackers Indicted on Spy Charges”. New York Times, Dec. 8, 1992, B, 13: 1. Finn, Nancy and Peter, “ Don’t Rely on the Law to Stop Computer Crime,” Computer World, Dec. 19, 1984, V18. Phrack Magazine issues 1-46. Compiled by Knight Lightning and Phiber Optik.

Shannon, L R. “ THe Happy Hacker”. New York Times, Mar. 21, 1993, 7, 16: 2. Sharp, B. “ The Hacker Crackdown”. New York Times, Dec. 20, 1992, 7, 18: 3. Sullivan, D. “ U. S. Charges Young Hackers”. New York Times, Nov. 15, 1992, 1, 40: 4. 2600: The Hacker Quarterly. Issues Summer 92-Spring 93. Compiled by Emmanuel Goldstein.