Delving into computer crime 18379

Technology, Computer

White-collar crime, specifically computer crime, is becoming more popular as computers become more readily available. Crimes using computers and crimes against computers are usually committed without fear of being caught, due to the detachment of the offender from the victim.

Computer crime is defined as, “ Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data.”(1). This includes both crimes using computers and crimes against computers.

The people who commit these crimes are of a wide variety. Cyber-criminals can be put in generally seven categories:

· Pranksters: These individuals perpetrate tricks on others. They generally do not intend any particular or long-lasting harm. A large portion is juvenile.

· Hackers: These individuals explore others' computer systems for education, out of curiosity, to achieve idealized social justice, or to compete with their peers. They may be attempting to gain the use of a more powerful computer, gain respect from fellow hackers, build a reputation, or gain acceptance as an expert without formal education.

· Malicious hackers (crackers): These individuals are intent on causing loss to satisfy some antisocial motives or just for fun. Many computer virus creators and distributors fall into this category.

· Personal problem solvers: By far the most common kind of criminal, these individuals often cause serious loss in their pursuit of a solution to their own

personal problems. They may turn to crime after conventional problem-solving methods fail, or they may see crime as a quick and easy way to solve their problems. “ They generally believe that the victim of the crime is rich enough to afford the loss and would not miss what was taken or used. Disgruntled employees, angry about being fired or not receiving a raise they felt they deserved, have also been known to “ even the score” with their company by disrupting their computer networks or program functionality fall into this category”(7).

· Career criminals: These individuals earn part or all of their income from crime, although they do not necessarily engage in crime as a full-time occupation. Some have a job, earn a little and steal a little, then move on to another job to repeat the process. In some cases they conspire with others or work within organized gangs such as the Mafia. The greatest organized crime threat comes from groups in Russia, Italy, and Asia. “ The FBI reported in 1995 that there were more than 30 Russian gangs operating in the United States. According to the FBI, many of these unsavory alliances use advanced information technology and encrypted communications to elude capture.”(7).

· Extreme advocates: Better known as “ computer terrorists,” these individuals and groups have strong social, political, or religious views and are intent on changing conditions by engaging in crime. Their crimes usually involve violence against people or property and are calculated to achieve a high level of publicity to bring attention to the terrorists' causes. “ To date, terrorists have rarely engaged in cyber crime, although the Red Brigades in

Europe came close by destroying more than 60 computer centers during the 1980s. Terrorist groups, especially the highly organized ones sponsored by rogue countries such as Libya and Iran, are likely to turn their attention to our fragile information, utility, and transportation infrastructures when their current methods lose their impact."(7). Such groups could plan an attack on a worldwide basis, using cryptography to communicate, and then carry out their acts through the Internet.

· Malcontents, addicts, and irrational and incompetent people: " These individuals extend from the mentally ill to those addicted to drugs, alcohol, competition, or attention from others, to the criminally negligent. In general, they are the most difficult to describe and the most difficult to protect against. We have no way of determining who is sufficiently irrational to trigger an attack against an organization or individual because of a perceived affront. We also have no way of predicting negligence. Criminal negligence is common in the abuse and misuse of computers. Programmers in New Zealand, for example, were convicted of criminal negligence when they failed in their duty to inform the captain of an airliner that they had reprogrammed his navigation system. He flew the plane into a mountain in Antarctica that, according to his navigation computer, was not supposed to be there, killing 80 tourists."(7).

Access to computer systems can be gained in many different ways. The simplest of these is direct access. Being the programmer, developer or specialist working with the system puts you in control of how the computer or network functions. Access can also be gained through a method called

cracking. Cracking is a method of finding and using somebody else's username and password. In order to crack a password, " you can make a good guess, try out a number of combinations, look for the combination (password) written someplace nearby or…one might try to find an alternate way into the system, a ' back door'"(2). Scanning is another way to " crack" information. Scanning is "[using] a computer program that automatically generates a sequence of phone numbers, credit card numbers, passwords or the like to try against a system entry test"(2). There are ways around scanning, such as putting a limit of attempts one gets to enter the correct password in the system entry test would stop the program from trying over and over again. An additional way one might gain access in through piggybacking. Piggybacking is " getting into a secured area by slipping in right behind someone who is cleared for access… [Piggybacking] can happen if the person using a terminal ahead of you did not log off properly, and her account is thus still active; you can go in"(2), basically it is using another person's access to as it were your own. The piggybacker then has access to all the past user's files and can be destructive if they choose and wipe out the account.

There are many different types of computer crimes, but there are basically two main categories, crimes against computers and crimes using computers. " Crimes against computers are usually based on the destruction of hardware and software or the theft of computer technology."(2). Many people get mad at computers for many reasons. Computers are based on human input, thus computers make mistakes. People sometimes take the anger that builds up, after a computer has made a number of mistakes, out

on the actual hardware such as: a computer monitor, tower, keyboard, or mouse. Demolished computers have been dropped, punched, kicked, and some even shot by a gun. Computer systems have also been mutilated and destroyed to destroy data and records. This is not the best method of destroying computer data. Although the system as a whole might be devastated, the data can sometimes be restored through special techniques.

Crimes using computers are more prevalent. There are numerous crimes that can be committed using computer, but they are not new crimes. The crimes were already in practice before it’s invention but new technology makes them easier to commit and provides less of a chance of getting caught. Money is the root of a lot of crimes, for instance, embezzlement is “ the act of stealing money that is entrusted to you”(1), or stealing from somebody that you work for. Banks are one of the best places to steal money from because, obviously, that’s where a large portion of money can be found. A great deal of the money that a bank oversees is not physical cash; it is numbers in computers. Many different and ingenious ways have been developed by computer criminals to embezzle money. The simplest form is to electronically transfer funds from someone’s account into your own. The possibility of being caught doing this is very high because it is noticeable and traceable. A method of embezzling called “ The Salami Technique”(2) involves slicing small amounts off of many different accounts (instead of just one big transfer) that won’t be noticed and putting the accumulating totals into one’s own account. There is also a “ round-off” technique where the amounts taken for oneself from each account are fractional and would otherwise kept by the bank as “ round-off errors”, such

as 3/10th of a cent but the small amounts build up over time. This can all be done with a patch or block of programming code added to the banks' accounting program during a single session. After the program is installed (or patched), all the criminal has to do is sit and wait. The program can be activated by an internal timer being set for a certain date and time.

Fraud broadens the computer criminals havoc-reeking horizons and is defined as " intentional deception"(2). Computers are probably the best means for trickery, especially through the Internet. When an individual logs onto the Internet through and ISP (Internet Service Provider), the only identity they are given is an IP (Internet Protocol) address. Nobody knows anything about the person using that terminal. They can fabricate any information they choose. Fraud includes, but is not limited to, creation of false accounts, using any accounts for which you are not entitled to use, destruction of records, et cetera.

The theft of information has also become a large problem in attempts to protect privacy. Many corporations and government organizations have extensive databases on a great deal of people. Information such as age, race, sex, social security number, address, telephone number, credit card information, and basically anything that has ever been known about a person is electronically stored and kept for reference. The problem with this data being stored electronically is that if the system is compromised, the data can be copied and stolen very quickly and can possibly be stolen over telecommunication lines. Phreaking is a kind of theft of services. Phreaking a process used to " access the telephone services illegally and run up

considerable calling bills for which they are never charged”(2). Using different tones, a computer can mock a request for a long-distance call, giving an individual free long-distance.

Cyberstalking, defined as “ The act or crime of willfully and repeatedly harassing another person in circumstances that would cause a reasonable person to fear injury or death because of expressed or implied threats”(1), is a relatively new problem. Irritating others over the Internet is something that commonly occurs, but the word “ repeatedly” placed in front of that statement can make a big difference. If someone is causing a nescience that interferes with ones’ professional or personal life it is considered stalking.

Catching the computer criminals is the tough part. There are “ Computer Crime Stopper” groups, hackers turned good, whose sole purpose and occupation is to track down and catch computer criminals. Tracking computer activity is a hard thing to do, especially over the Internet. There is no “ trail” left for the criminal to be followed by. Usually the only thing crime-stoppers have to go on are the IP addresses and telecommunication lines to trace to find the origin of the signal, but the perpetrator is normally long gone by the time authorities arrive.

Prevention is a crucial part in protecting the computers of today. Through secure servers, which are “ special computers [that] provide secure connections between networked computers and outside systems,”(4) companies protect credit card and other personal information of their clients. Encryption is a method of “ encoding”(4) data using a set of key (a mathematical formula), which is then sent to the receiving party. They have

the “ decoding”(4) key to transform the data back into understandable data. Encryption works very well, as long as the key doesn’t fall into the wrong hands. Firewalls, “ a safety computer placed between a network and outside systems”(4), can deter break-ins from external systems using usernames and passwords, but as we know they can be cracked with some effort.

The current laws and regulations against crime do not apply to computer crimes. Although some laws are twisted and contorted to apply to new situations as they arise, I feel that new legislation needs to be put into place to apply to the crimes and criminals. Cyberstalking is a good example of a computer crime that needs it’s own legislation to govern what is to be considered stalking and what are not over the Internet. Stalking without a computer is clearly defined, both what stalking is and what the penalties are for committing it, but communication over the Internet isn’t as clearly regulated. Are 2 E-Mail’s to a person that didn’t want them considered stalking, and if so then why isn’t unwanted E-Mail from organizations considered soliciting? Statues need to be presented to clearly outline what is wrong and what is okay. Instead of trying to apply unrelated laws to fast-growing criminal opportunities, we should establish a basis for which all computer crimes can be tried and prosecuted.

“ It has been said that the Internet is the first empirically lawless domain of modern life. Even with the most carefully crafted legislation, enforcing a law in a virtual community creates unique problems never before faced by law enforcement agencies.”(6). Since the “ means” of committing the crimes is different, should we consider different punishments? In the past, convicted

computer criminals have served generally light terms for their crimes. Shouldn’t embezzlement done by a machine, which a human caused it to do, be the same as embezzlement done directly by the hands of a human? I guess one could say that we are lucky that ALL crimes can’t be committed over a computer, at least not yet.

Bibliography

(1) Bowen, Mace. “ Computer Crime.” 9/14/99. http://www. guru. net/. Visited: 10/28/00.

(2) Edgar, Stacey L. Morality and Machines: Perspectives on Computer Ethics. Sudbury: Jones and Bartlett Publishers, 1997.

(3) Jenson, Barbara. Cyberstalking: Crime, Enforcement and Personal Responsibility in the On-line World. New York: Wiley Computer Publishing, 1996.

(4) Parker, Donn B. Computer Security. CD-ROM. Encarta Encyclopedia 2000. Microsoft Corporation. 1993-1999.

(5) Parker, Donn B. Fighting Computer Crime: A New Framework for Protecting Information. New York: Wiley Computer Publishing, 1998.

(6) Tribe, Laurence H. The Constitution in Cyberspace. New York: Warren & Computer Professionals, 1991.

(7) U. S. Dept of Justice. “ Cyber Crime.” 5/23/00. http://www. cybercrime. gov/. Visited: 10/27/00.

Word Count: 2254