Computer ethics and crime 591

Technology, Computer

Introduction

Legality, piracy, ethics, effects, moral dilemmas, motives, age, involvement, types -

encryption are all main issues in Computer Crimes in todays world. How do we determine

someone fate? Computer crime has become such a hot topic in the media since the middle

of the 1980's. By now most of us would have probably recognize the names of some of

the prominent " hackers" such as Kevin Mitnick or Robert Morris, which I will touch upon

their crimes. These hackers or more appropriately " crackers" have been both vilified and

herofied by the media and the computer field. Some of these criminals have been made

out to be modern day Robin Hoods, or cyberpunks or whatever. I however disagree with

them, and feel as a member of the computer community their actions are irresponsible.

Kevin Mitnick is a well knowncomputer criminal who was apprehended with the

aided of " Cybersleuth" Tsutumo Shimomura, whose computer was one of the many that

Mitnick invaded. He had always been in trouble with the law for computer related crimes.

He was first convicted and was declared to be addicted to computers. Part of the

stipulations of his parole was that he not have access to computers. It was his return to

computer use that brought the law against him, but he was not captured again until after

invading Shimomura's computer. Mitnick had apparently invaded computers across the

nation, stealing millions of dollars worth of corporate trade secrets, in addition to over

20, 000 credit card numbers.

Robert Morris was the author of the infamous Internet " worm" that brought the

Internet to a standstill back in 1988. Morris a highly knowledgeable first year graduate

student at Cornell University authored this worm program which exploited many security

flaws in the UNIX operating system to spread throughout the Internet. Reactions to his

worm are greatly varied. Some claim that this act was unlawful, irresponsible, and

negligent. However, other have heralded his release of the program as a way to bring

national attention to the security flaws inherent in the UNIX operating system.

Legality

The United States government has proposed that a compromise that would allow

people to use encrypted devices, but still allows the government to break the codes if

necessary. Essentially, an encryption chip, the clipper chip, would be placed into devices

that need secure data transmission. The keys to decoding the encrypted message would

be kept in escrow by two separate government agencies. Each agency would contain half

of the key to prevent abuse. Law enforcement agencies would be able to obtain the keys

by obtaining a warrant.

The current body of laws existing today in America does not apply well to the

Internet. Is the Internet like a bookstore, where servers cannot be expected to review

every title? Is the Internet like a phone company who must ignore what it carries because

of privacy? Is it like a broadcasting medium, where the government monitors what it

broadcasts? The trouble is that the Internet can be all or none of these things depending

on how it's used. The Internet cannot be viewed as one type of transfer medium user

current broadcasting definition.

Jim Exon, a democratic senator from Nebraska, wants to pass a decency bill

regulating the Internet. If the bill passes, certain commercial servers that post pictures of

unclad beings, like those run by Penthouse or Playboy, would of course be shut down

immediately or risk prosecution. The same goes for any amateur web site that features

nudity, sex talk, or rough language. Posting any dirty words in a Usenet discussion group,

which occurs routinely, could make one liable for a $50, 000 dollar fine and six months in

jail. Even worse, if a magazine that commonly runs some of those nasty words in its

pages, The New Yorker for instance, decided to post its comments on-line, its leaders

would be responsible for a $100, 000 fine and two years in jail. Why does it suddenly

become illegal to post something that has been legal for years in print? Exon's bill

apparently would also " criminalize private mail," ... " I can call my brother on the phone

and say anything -- but if I say it on the Internet, its illegal".

Congress, in their pursuit of regulations, seems to have overlooked the fact that

the majority of adult material comes from overseas. Although many U. S. government

sources helped fund Arpanet, the predecessor to the Internet, they no longer control it.

Many of the new Internet technologies, including the World Wide Web, have come from

overseas. There is no clear boundary between information held in the U. S. and

information stored in other countries. Data held in foreign computers is just as accessible

as data in America, all it take is the click of a mouse to access. Even if our government

tried to regulate the Internet, we have no control over what is posted in other countries,

and we have no practical way to stop it.

Piracy

Software piracy is a very large problem in the software industry. Millions of

dollars are lost in sales yearly by software corporation because of it. In addition to the

loss of sales, software piracy also aids in the spread of computer viruses. There have been

a number of occurrences of viruses that were designed to show how rampant piracy

actually is. Here is two examples of software piracy; Aldus Peace Virus and the Pakistani

Brain.

The Aldus Peace Virus was a harmless virus that was inserted into a popular

computer game that displayed a message of peace to Macintosh users on March 2, 1988.

Richard Brandow acknowledged that he had written the message and that his intention

was to display how widespread software piracy had become.

The Pakistani Brain Virus was designed by two brothers, Amjad Farooq Alvi and

Basit Farooq, who ran a software company to protect their software from piracy. They

entered it into programs so that they would know who pirated their software when they

called for the vaccination. They also inserted this virus into American copyrighted

software that was being purchased in Pakistan because they believed that by purchasing

American software that wasn't protected by copyright laws in Pakistan that people were

pirating that piece of software and should be punished.

Ethics

This is a touchy subject, there are many various meanings; Unethical means not

conforming to an appropriate personal standard of conduct, Not ethical means not

violating an appropriate personal standard of conduct, No ethics means no appropriate

personal standard of conduct was involved or the action was clearly illegal.

Advancements in computer and data communications technology have resulted in

the need to re-evaluate the applications of ethical principals and establish new agreements

on ethical practices. The application of ethics information science, technology, and

business is more difficult than in other disciplines for several reasons. Computer and data

communications alter relationships among people. Data communications take place

without personal contact, without the visual and aural senses to help convey meaning.

Moreover, the paperless society, in which information is transmitted at electric speeds,

functions side by side with the paper-based society, where information is shared at a snail's

pace. Conveying one's intentions in a letter, which can take days to reach the recipient, is

very different from instantaneous electric transmission because of how quickly the

recipient may act on them. Communication occurs so quickly that one may not have time

to consider the implications of the information before it has been sent and received.

Information in electric, magnetic, and optical form is far more fragile than

information on paper. Computers and data communications systems provide for high-

speed, low-cost processing, communication, copying and printing of intangible intellectual

property. This capability introduces new factors in decisions about property rights,

residual rights, plagiarism, piracy and violation of privacy. Negative events happen so

easily, sometimes without the initiators even considering the consequences, that ethical

issues are intensified. Freedom of expression is greatly levered and magnified to the

extent that far more good may be done with creation, use and dissemination of

information. Yet it follows that the consequences of unethical acts are equally magnified.

Effects

Believe it or not computer crimes, I believe do have some positive effects. That

the U. S. violent crime rate drops 10 percent from last year. The survey, issued by the

department's Bureau of Justice statistics, found an estimated 2. 7 million violent crimes last

year, down from 3. 0 million in 1995. according to the survey, property crimes, such as

household burglaries and motor vehicle thefts, recorded an 8 percent decline last year.

The victimization rates in 1996 are the lowest recorded by the survey since its inception in

1973, Jan Chaiken, the director of the statistics - gathered agency, said.

People tend to be finding different ways to commit crimes, through computers, in

their offices at work to the computers at their homes. I think it is the lesser of the two

evils, I would personally rather have someone break into my bank account than my home.

That way their is no physical endangerment to my family members and myself. I approach

the situation this way, damage through a computer would not hurt us physically 90

percent of the time, and physical damage can never be fixed 100 percent and money can

always be replaced, not a human life.

Morals

The general public all have common truths that apply to everyone's behavior. We

all know that the ends do not justify the means, and that two wrongs don't make it right

and the notion " everyone else is doing it". Most people have tried to justify an action not

the answer nor an excuse for harmful actions caused.

Motivations

Much of the unauthorized entry into computer systems is done by young computer

enthusiast who are seeking to display and test their computer skills. Some claim to try to

penetrate systems so that they can learn how to better protect their own systems. These

types of invasions have led many skilled hackers to find their way into employment as

security consultants. There have been some cases in which people have written viruses or

broke into and damaged computer systems as a means of punishing individuals for

committing wrongs. Some invasions occur just because the intruder wants to look around

the system and see what is there, sometimes leaving a calling card message behind to let

the owner know that they penetrated into their system.

Philosophy is where the hacker ethic comes into the discussion. Many hackers and

computer users believe that all information should be free and available to the public. So

they break into protected systems to release hoarded information. The Idle system

argument claims that most computers sit idling by wasting cycles. Therefore it is

acceptable for hackers to break in and use these wasted cycles because it benefits the

overall society by providing more people with access to computing power. The student

hacker argument addresses the issues around the learning process of breaking into

systems. People claim that by breaking into systems, one can learn a great deal about

computers and therefore these types of educational break-ins are not unethical.

There is also a threat that people will break into computer systems to cause

sabotage or aid in terrorism. There has been little evidence of such activities released to

the public, but it is known that both the CIA and NSA are experimenting with computer

viruses as strategic weapons. I find this to be slightly ironic because the United States is

one of the only nations that could actually be crippled by such a virus.

Age

As we mature, however, ethics take on a new meaning and importance, especially

as we begin a professional career. Computer education now begins in grade school, it is

no longer a restricted technical specialty, learned only as a part of on-the-job training or in

an engineering or mathematics graduate program. Computers have become as

commonplace as telephones. The related ethical issues have thus become more

democratically defined. More people have more to say about computer ethics simply

because so many more people are computer-literate. On the other hand, the diffuses of

the impacts and the wide distribution of the technology mean that recognizing impacts, let

alone solving an ethical dilemma, is much more difficult.

Involvement

This type of computer crime and abuse is one which attaches a great deal of

attention from the media. It is in this area that many " hackers" have achieved Robin

Hood status. This area encompasses a broad range of criminal activity, the law

concerning which is still being shaped. Old law doesn't apply well here because of the

problems surrounding electric data as property. Many states have begun to try to expand

property definitions to include electric data, use of computers to commit, aid or abet the

commission of crime, crimes against intellectual property, knowing unauthorized use of

computers, unauthorized copying of electronic data, the prevention of authorized usage of

computers and electronic data, unlawful acquisition and prevention of use of computers.

Encryption

With the heightened awareness of the lack of privacy that exists in cyberspace, the

many members of the computing community have embraced the usage of encryption.

However, encryption has many legal barriers that restrict it. The United States

government fears that the widespread usage of encryption by people because it fears that it

will not be able to crack encrypted transmissions and will not be able to enforce law as

effectively as it has in the past. It also fears that the exportation of advanced American

encryption devices and techniques poses a significant risk to national security. This is why

encryption devices and algorithms are classified as munitions.

Some current examples in the encryption field are PGP and RSA encryption.

Author Phil Zimmerman was investigated by the United States government for violating

export laws, by making Pretty Good Privacy(PGP) available on the World Wide Web

where it was down loaded to sites outside of the United States. RSA encryption is often

considered a standard in software that uses encryption techniques. RSA can be written in

4 lines or PERL code and could easily be exported. An industry problem arises with RSA

because American companies that use RSA encryption in their software, have to use less

secure encryption techniques in the software they export out of the United States and thus

hurts their sales because foreign consumers are aware of the decrease in security.

Conclusion

Although a computer is not unethical, certain applications of computer maybe.

Moreover, replacing a manual activity with an automated device does not change the

ethnically of the activity. Using a computer as a marketing tool, for example, is not

unethical. When the device being used is hidden, however, ethically becomes more

difficult to judge. A hidden device used in a accepted relationship is unethical, but

enhancing one's intellect with a device in a computer game or else where, as long as such

use does not violate the commonly understood rules or laws is ethical. Given our

increasing technology capacity to develop ever more powerful computers, the

controversy on these issues can be expected to increase for many years to come.

Yet, there is a great deal of potential damage to be done by computer criminals

especially as we move into a more computer dependent age. It is up to us to decide what

we find ethical in regards to Computers and electronic information and resources should

be unrestricted because we have no property claims upon it and it will increase overall

efficiency. But there are also those who argue against this type of electronic socialism.

The laws are currently being shaped around us, but regardless of this there will always be

computer crime. What we must really decide is how to punish it. How should intent

factor into computer break-ins? Should all break-ins be considered equally unethical or

would those where the intruder only intended to have a look around be seen as more of a

misdemeanor than a felony? In conclusion, the field of computer crime will indeed be an

interesting passage to follow.