Compare and contrast the four different categorizations of computer crimes.

CCSI 330 Final Project

Mike Mateja
D03172035
12/11/2009
On October 29, 1969, a UCLA student supervised by a Professor sent the first message through a host to host connection (ARPANET -- The First Internet, 2009). This was the birth of the Internet. The Internet changed the way we work, shop and even socialize. It has also given criminals a new medium to commit crimes. As the Internet evolves over time more users get plugged in everyday. We will become more susceptible to falling victim to criminals tactics even from the comfort of our own home. The crimes that these online criminals commit have been divided into categories. There are four categories of computer crime. First, Crimes committed using a computer as a target. Second, Crimes committed using a computer as a tool. Next, Crimes committed as incidental to computer use. Finally, Crimes associated with the prevalence of computers. It is difficult to distinguish between these four categories because when a cybercriminal is found they usually have broken more than one. Yet, there are still differences.

When a criminal commits a crime using the computer as a target, two steps must happen. First, the criminal must gain access to the computer. This is called intrusion. Second, he must deny the owner service or data stored on that computer. Intrusion by itself does not deprive the owner of service or data (Taylor et al, 2006). Intrusion does, however, question if data has remained unaltered. If data is altered then intrusion has definitely occurred. The difference between intrusion and data alteration is also defined by the intent of the hacker. Intrusion is made possible when a hacker, makes use of social engineering skills to ascertain passwords, logins and even policies from an intended target. Then a hacker can use this acquired information to intrude upon another computer. In order to commit the crime of using a computer as a target, he must deny service or data to the owner. The act of making a copy of data counts as denying data because it denies the owner the rights of privacy of this data. One
method to cause denial of service is to infect the intruded computer with a virus to cause the
computer to be remotely controlled. Botnet computers have recently been a problem in the
United States. According to John Shiffman of the Philadelphia Inquirer, he quoted Robert
Mueller if the FBI saying “Today, Botnets are the weapon of choice of cyber criminals.” John
Shiffman also reported a story about a hacker from New Zealand, code named “Akill”, who was
responsible for infecting over a million Botnet computers. Akill used these Botnets to attack
servers located at the University of Pennsylvania (Shiffman, 2007).

The definition of when a computer is used as an instrument of a crime is best explained
by our textbook. Our book states that “just as a burglar uses a crowbar, criminals can use a
computer.” (Taylor et al, 2006) When the computer instrument is “played” criminals use it to
commit acts of theft, fraud and harassment. An article I read identified the type of person who
would be a target for a victim of a computer crime as someone who is naive, financially
unstable and believe they can get rich quick. On the other hand the perpetrators of computer
crimes are most likely disgruntled employees, teenagers or business rivals (Upchurch, 2009).
One example of a popular crime a computer can be an instrument for is called the “Salami
Slice” (Upchurch, 2009). Chris Conrad a reporter for Mail Tribune, just this last thanksgiving,
reported a story about a motorcycle shop employee who wanted a slice of some one’s else’s
salami. This employee altered computer records to make it appear as though customers
returned merchandise and then pocketed the money. Only taking $40 to $50 at a time it added
up to $7000 (Conrad, 2009).

I can understand the motivation for these crimes. Disgruntled employees wishing to
“stick it” to the boss or money troubles driving an employee to take advantage of a situation,
but cyber bullying is a crime which is acted by pure maliciousness. USA, Today ran a story about a Missouri women who impersonated a 16 year old boy in order “to torment, harass, humiliate and embarrass a juvenile”. The women began to flirt then harass a 13 year old girl, also from Missouri. One the final messages sent told the 13 year old that “the world would be better off without her”. This harassment had leaded the girl to hang herself. The case was characterized as “cyber bullying”, the women was convicted and serving five years in prison (William, n.d.).

These types of crimes are similar because they require a criminal who has been taught or has learned skills to hack in to these systems. These criminal were knowledgeable in technology and successfully used social engineering tactics to get what they needed. Anonymity is a motivator for committing these two types of crimes. The belief that the criminal cannot be traced or identified might allow them the courage to attempt an intrusion. When people feel like they’re not being watched, their true side is revealed.

In contrast between the crimes of using a computer as a target and crimes using a computer as a tool is that the intent of the user is different. When the crime of using a computer as a target is perpetrated, the intent is exploratoral in nature rather than malicious. Criminals in this mind set are more interested in how the system works rather than how to take it down. When a computer is used as an instrument of a crime, the intent is malicious. Harassment, threats and blackmail over a computer interface is more attractive to a cybercriminal and also scarier for the victim because of the belief of anonymity. The most important issue for the victim to remember is to report and document the crime. The more information we can acquire about an attacker the faster they can be caught.
When a Computer is used as incidental to a crime, this means that a criminal has already committed a non-computer crime but has been using a computer to increase his efficiency in performing this crime. The added use of the computer to solicit additional business and affect a larger group of people is the basis for this crime. Some examples of how a computer can be incidental to a crime are money laundry, prostitution rings and child pornography enterprises. Child pornography is considered an incidental computer crime because the first crime is taking the pictures. The computer crime is the fact that with the help of the internet, a pedophile can reach a larger market to sell and distribute pictures. As long as pedophiles have a market to distribute on, children are at risk. One of the worst and most recent child pornography cases was committed by a 54 year old male architect in Cork City, Ireland. This last November, he pleaded guilty to having downloaded 13,845 pornographic images of children between the ages of one and six. His sentence is pending an 18 month psychiatric treatment at Granada institute in Dublin (Southern Correspondent, 2009).

Crime that is associated with the prevalence if computers account for the violation of intellectual property rights, identity theft and even physical component theft. In plain English, these crimes are cause by the existence of computers. Physical component theft has decreased since the advent of the home computer age because of two reasons; first, components have become less expensive. Second, it is possible that less people are reporting it. This is due to poor record keeping of serial and model numbers (Taylor et al, 2006).

The violation of intellectual property rights occurs when someone “copies or distributes copyrighted material without the consent of the copyrighted holder” (Adamsick, 2008). In my
opinion, the fact this is a crime is still debated in public circles. Napster and Lime wire are two very popular programs that can assist users with committing this crime.

The advancement of technology has always stayed one step in front of the law. This remains true in identity theft, also. In 2006, there were 15 million occurrences of identity theft (Burkhalter & Crittenden, 2009). I believe this is made possible by the easy of availability of public records online. Also, a possible factor is the amount of data that continues to float around in the cloud of the internet. It would not take long for a criminal to compile a list of data relevant to any of us. Referencing your address in Google earth, would even provide actual picture of your home and your car in the driveway. In order to protect ourselves, we must be mindful of what and whom we share data with.

Between crimes committed as incidental to computer use and crimes associated with the prevalence of computers, they share similarities because both deal with theft. But differ because of the actual data that is actually stolen. Stealing data or violating a copyright, when a criminal pursues to commit the theft of intellectual property rights or of an identity is just as much a crime as stealing money from a register or mugging someone on the street. In contrast though; these two types of computer crime differ because of the level of anonymity of the victim. When a crime is committed or intellectual property rights violated, it is easy for the thief to assume, they stole from a big company who would not miss the money, rather than in theft or harassment which is a, one on one, malicious crime.

In conclusion, my research has taught me some abstract and concrete aspects of computer crimes. The abstract aspects have given me a sense of where computer crimes originated and that they are always one step in front of the law. The concrete details of
computer crimes are the fact that laws need to be constantly updated along with technology in order to be relevant to society’s expectations of security.
References


