White collar crime: computer fraud

Law, Crime

White Collar crime has been Identified by Edwin Sutherland as “ A crime committed by a person of respectability and high social status in the course of his occupation" (Sutherland, 1939) White Collar crimes are serious, but non-violent crimes that usual deal with stealing money or other material items. Majority of the time they involve scams and an degree of high intelligence is needed to actually commit and not get caught.

White collar crime has victims just like violent crimes and the victim may be affected for life. A few examples of a white collar crime would be, embezzlement, Copyright infringement, money laundering, bribery, computer crimes, and different kinds of fraud. Since technology has come into play many issues have come to surface and the crime rates have increased causing one particular branch of white collar crime known as computer fraud.

Computer fraud is where computer hackers steal information sources contained on computers such as: bank information, Credit cards, and proprietary information. Bank information consists of amounts, pin numbers, debit card numbers and information like that. It is obvious as to why computer fraud is a dangerous type of white collar crime committed; it affects thousands of people every day. There are many types of cyber crimes that are related to computer fraud.

Hacking into networks via Phishing and fake website, financial crimes such as siphoning of money from banks, credit card frauds, money laundering, online gambling, Intellectual property crimes such as theft of computer source code, software piracy, copyright infringement, trademark violations,

Harassments such as cyber stalking, cyber defamation, indecent and abusing mails, Launching of virus, worms and Trojans, Cyber attacks and cyber terrorism. As a general matter, copyright infringement ccurs when a copyrighted work is reproduced, distributed, performed, publicly displayed, or made into a derivative work without the permission of the copyright owner. The amount of Copyright infringement cases have increased dramatically lately with sites like Limewire, Frostwire and similar websites pirating music has become easy and accessible for anyone anywhere in the world. Limewire, the biggest of the file sharing websites was recently shut down on October 26, 2010.

According to the injunction, Limewire “ intentionally encouraged infringement” by Limewire users, it is used “ overwhelmingly for infringement” and it knew about the “ substantial infringement being committed” by its users. The government finally got enough information to close it down for good, but another site will surely take its place. Computer hacking has also increased. Computer’s automatically store numerous files that contain your most sensitive data like your address, name and even credit card information. Spyware is often used by hacker’s and legitimate companies.

Once it is installed into a computer it has the ability to monitor a user’s activity and collect information without their knowledge or consent. Other approaches include a system called phishing in which the hacker sends out a bunch of emails, and take advantage of the person by stealing credit card information and other things like that. The email may claim it’s from a bank

and look legitimate, but once you send your information through the site it has now been given to someone to steal money or purchase numerous items causing horrible credit and/or other things like Identity theft.

Identity theft is the biggest problem as a result of computer fraud. This process is when someone basically steals individual’s identity. is a form of fraud or cheating of another person's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. The victim of identity theft can suffer adverse consequences if he or she is held accountable for the perpetrator's actions. Computer crime can become an obsession.

Such was the case for Kevin Mitnick, a man federal prosecutors described prior to his arrest as the most wanted computer hacker in the world. In the early 1980s, as a teenager, Mitnick proved his mettle as a hacker by gaining access to a North American Air Defense terminal, an event that inspired the 1983 movie War Games. Mitnick gained access to computer networks through telecommunications systems. In violation of federal law, he accessed private credit information, obtaining some 20, 000 credit numbers and histories.

Other break-ins by Mitnick caused an estimated $4 million in damage to the computer operations of the Digital Equipment Corporation. The company also claimed that Mitnick had stolen more than one million dollars in software. Mitnick was convicted, sentenced to one year in a minimum-security prison, and then released into a treatment program for compulsive-

behavior disorders. Federal investigators tried to keep close track of him during his probation, but in November 1992, he disappeared.

Authorities caught up with his trail when Mitnick broke into the system of computer-security expert Tsutomu Shimomura at the San Diego Supercomputer Center—a move that was clearly intended as a challenge to another programming wizard. Mitnick was arrested and was charged on 23 federal counts. He plea-bargained with prosecutors, who agreed to drop 22 of the counts in exchange for Mitnick's guilty plea for illegally possessing phone numbers to gain access to a computer system. Mitnick was sentenced to eight months in jail.

Mitnick's case illustrates the difficulties that legislatures and courts face when defining and assigning penalties for computer crime. Using a computer to transfer funds illegally or to embezzle money is clearly a serious crime that merits serious punishment. Mitnick broke into numerous services and databases without permission and took classified information, in violation of federal laws; however, he never used that information for financial gain. This type of behavior doesn’t occur outside of cyberspace for example, people do not break into jewelry stores only to leave a note about weak security.

Some instances of computer crimes demonstrate the way in which small computer files that require relatively little effort on the part of the perpetrator can cause millions of dollars' worth of damage to computer networks. In March 1999, David L. Smith of New Jersey created a virus that lowered the security levels of certain word-processing programs and caused infected computers to send e-mail messages containing attachments with

the virus to e-mail addresses contained in the infected computer's e-mail address book.

The virus was activated on an infected computer when the user opened the program. Smith posted a message on March 26, 1999, to an Internet newsgroup called " Alt. Sex. " The message claimed that if a user opened an attachment, it would provide a list of passwords to pornographic websites. The attachment contained the virus, which became known as the " Melissa" virus. Smith was arrested by New Jersey authorities on April 1, 1999, but not before the virus had infected an estimated 1. million computers and affected one-fifth of the country's largest businesses. The total amount of damages was $80 million. Smith pleaded guilty to state and federal charges. He faced 20 months in a federal prison and a fine of approximately $5, 000 for his crime. He faced additional time in state prison. According to U. S. Attorney Robert J. Cleary, " There is a segment in society that views the unleashing of computer viruses as a challenge, a game. Far from it; it is a serious crime. The penalties Mr.

Smith faces—including potentially five years in a federal prison—are no game, and others should heed his example. " In 1986 Congress passed a law called The Computer Fraud and Abuse Act which was intended to reduce cracking of computer systems and to address federal computer-related offenses. It governs cases with a compelling federal interest, where computers of the federal government or certain financial institutions are involved, where the crime itself is interstate in nature, or where computers are used in interstate and foreign commerce.

It was amended in 2002 and in 2008 by the Identity Theft Enforcement and Restitution Act. Subsection (b) of the act punishes anyone who not just commits or attempts to commit an offense under the Act, but also those who conspire to do so. The following are some primary indicators that a computer may be infected: The computer runs slower than usual, the computer stops responding, or it locks up frequently, the computer crashes, and then it restarts every few minutes, the computer restarts on its own.

Additionally, the computer does not run as usual, applications on the computer do not work correctly, disks or disk drives are inaccessible, or the computer cannot print items correctly Prevention methods against Computer fraud and cyber crimes in general would be to never give out valuable/private information via email, websites, or other things. Effective Anti-Virus software should be installed on your computer, so you can be aware of any intrusive files, Trojans or worms that may be trying to access your computer files. The best thing to do is to be smart.

Never give your private information to anyone over the internet or even to anyone in general. Computer Fraud and Cyber crimes are accelerating at an alarming rate. Many things are being done to prevent these types of white collar crimes, but as soon as the government figures out everything hackers, and the other criminals, are already ten steps ahead of them. Also when governmental agencies finally figure things out technology is already advancing and new ways to commit these crimes increase. As long as computer’s are around and technology keeps improving the crime rates are going to escalade and will continue to exist.

References

http://www. spamlaws. com/computer-fraud. html

http://legal-dictionary. thefreedictionary. com/Computer+fraud

http://www. referenceforbusiness. com/encyclopedia/Clo-Con/Computer-Fraud. html