Example of computer crime essay

Business, Company

A computer crime is defined as any form of crime that involves a network and a computer. Early computer crimes often involved physical damage to computer systems and subversion of the long-distance telephone networks. The earlier periods, 1960s and 1970s, were not common with computer crimes. Actually, the incidents were mere pranks played on the computer systems. There were also few laws against such activities and that is the reason why they were never viewed as crimes. This paper therefore discusses the history and origins of computer crime.

According to Kabay (2008), computer crime began as early as the 1870s with the early telephone system. Typically, the teenage boys who were employed by telephone companies would play pranks. They frequently crossed lines and intentionally became rude to subscribers. This would definitely interfere with the telephone network. This violation escalated into the 1950s when individuals found different ways to scam phone companies into receiving uncharged long distance` phone calls. In fact, it was during this period that witnessed a computer crime referred to as phone phreaking. Since then, computer crime has directly progressed just the same way that complexity of the computer systems are progressing. A perfect example is the Equity Funding Fraud of 1973 (Kabay 2008). This kind of fraud demonstrated how a company used their computer systems to produce fraudulent profit numbers to fool potential investors. It resulted in a type of computer crime referred to as data diddling. Data diddling is the illegal or unauthorized data alteration. The changes can occur before and during data input or before output. Such cases have since included bank records, inventory data, payrolls, school transactions and unauthorized alteration of school records.

The 1970s witnessed the introduction of salami fraud. Salami fraud basically constituted individuals who used computer systems a small, undetectable amount of money from numerous individuals. In essence, in the salami technique, criminals steal money or resources a bit at a time. An example of salami fraud came into the public view in 1993 when a Value Rent-a-Car company scammed each of its customers out of a range of $2-$15 by deceiving them about the size of the gas tanks. This allowed the company to charge extra for cars returned without a full tank (Kabay 2008).

The pivotal year in the whole history of the world's computer crime was in 1981. Significant developments in computer crime took place during this time. In fact, the development in computer crime was attributed to the sudden decrease in computer prices. The drastic fall in prices of computers has eventually put many households in a position to own one. Unfortunately, the increase in computer purchase comes with computer crimes. This is because many of the people who own computers today are ignorant of the safety measures they can use to protect themselves as well as their privacy (Kabay 2008).

In 1980s, the computer crime that rocked the world was the invention of logic bombs. According to Kabay (2008), a logic bomb is a program which has been intentionally modified to produce results when certain conditions are met that are unexpected and unauthorized by legitimate users. The logic bombs were either within a standalone program or were part and parcel of worms. A notorious time bomb is that of a of PC virus from the 1980s, Cascade, that made all the characters fall to the last row of the display during the last three months of every year (Kabay 2008).

As a result of the higher rate of progress of computer hacking, clubs such as the Chaos Computer Club of 1981 emerged. These clubs composed numerous hacking members that never posed any harm. Instead, they hacked computer systems, including high ranking business computer systems, to demonstrate to other companies where the flaws in their computer security existed. In fact, it is this type of club that paved the way for many organizations that carried out the similar tasks (Kabay 2008).

An infamous computer hacker who has dabbled in all types of different computer hacking throughout his life, including phone phreaking and data diddling is Kevin Mitnick. Kevin began his hacking career at an early age. At the age of 16, he hacked a computer system belonging to Digital Equipment Corporation called The Ark in which he stole all the company's information. It was this move that gained him recognition in the hacking community and which eventually led to his conviction in 1988. After 12 years in prison, he was released on a three year probation period in which he escaped from the law and eluded the police for 2 years, surviving on money he gained from hacking various computer systems around the world, cloning cell phones, and copying valuable software. After his apprehension in 1995 and serving five years in prison, the government realized the value of his extensive knowledge and now owns his own security consultant company which works with the United States Government (Greene 2003).

Generally, it is evident that the progression in computer hacking began with childish pranks, evolved to theft and fraud, and later moved to a means of countering crime. Although there is an increasing amount of identity theft, computer fraud, and internet crimes, there are also computer hackers who

use their knowledge to help protect innocent people from being victims of these crimes.

Work cited

Greene, T. C. Kevin Mitnick's Story. The Register. (2003).

Kabay. M. E. A Brief History of Computer Crime: An Introduction for Students (2008). Web. 10 October, 2012.