Cyber Crimes: The Essence And A Brief Summary

Abstract

Over the last thirty years computers and the internet have become essential for the day to day activities of the average American. Nowadays, thanks to mobile devices, people are constantly connected online and access to their personal information is just a few clicks away. The convenience of having easy access to so much data also attracts criminals that seek to enrich themselves by exploiting the vulnerabilities of the systems connected to the internet. A report by the Council of Economic Advisers revealed that on average a firm experiences 130 security breaches a year (2018). Since internet crimes are so pervasive and affect a wide range of the population, it is important to understand the types of crimes that the average internet user might be exposed to. In the first section of this research paper, the various types of cyber-crimes are introduced. Their most common mode of operation and the vulnerabilities they exploit are presented in the second section. In the third section, the legal consequences of those crimes are explored. Finally, in the last section, concluding remarks are presented.

Cyber-crimes

The advent of computers brought with it the ability for people to be closer to each other. Distance no longer held sway in a relationship as everyone became just a phone call away. With this being the case, the issue of crime has begun to evolve. Nowadays, thanks to mobile devices, people are constantly connected online and access to their personal information is just a few clicks away. The ease at which technology has advanced has made it in such a way that almost everybody has a computer. Cybercrime has an unpredictable future judging from the trends where the culprits always end up a step ahead of the authorities. The convenience of having easy access to so much data also attracts criminals that seek to enrich themselves by exploiting the vulnerabilities of the systems connected to the internet. Cybercriminals always come up with a new way of committing the crimes. Authorities must increase their skill levels if they hope to catch up with cyber-crime committers. Cybercriminals seem always to find a new way of defrauding people and scamming them for their money. Regions like Asia have a high amount of cyber-crime based on the vast populations and the exposure that this massive population has to the computer systems. Close to eighty percent of the population have access to computers. A look at the growth of cyber-crimes shows that there is a high chance that it would continue growing. People depending on current laws and technical protection is no longer enough protection against cyber-crimes. Therefore, due to the technological advancements and lack of technological know-how in recent years, the amount of people that have fallen prey to internet-related crimes continues to rise.

Cyber-crime is an illegal activity conducted using a computer. Computer crimes are crimes committed with the aid of a computer. A cyber-crime refers to a situation where an authorized person gains access to data without the permission of the administrator in charge of the system. Any criminal activity that occurs with the aid of a computer over the internet is thus a cyber-crime. This aspect includes the hardware device as well as the internet. The computer and the internet serve as tools that facilitate and allow the occurrence of crime. Cyber-crime covers a range of offenses. These include cyberstalking, child pornography, unauthorized access,

forgery and fraud among others. With the changing world and increasing technology, the computer has become one of the main tools that people use to commit criminal activity. This kind of crime does not necessarily involve the loss of data on the computer or even the change of data on the computer. Due to the introduction of computers it has become easier to commit crimes from the comfort of your home.

The history of crimes committed with a computer is plain to see. In 1971, John Draper created a whistle that was used to make long distance phone call by copying computer tones at the time. In 1973, a New York teller used a computer to embezzle $2 million dollars from the bank he worked at. In 1978, the first electronic bulletin board that included free hacking tips was created. In 1986, The United States Congress passed a bill called the Computer Fraud and Abuse Act making hacking and theft illegal. In 1990, The Legion of Doom and Masters of Deception, two cyber-based gangs, engage in online warfare. They actively block each other's connections, hack into computers and steal data. These two groups were large-scale phone phreaks famous for numerous hacks into telephone mainframe infrastructure. In 1994, The World Wide Web is launched, allowing black hat hackers to move their product info from the old bulletin board systems to their very own websites and a student in the UK uses the information to hack into Korea's nuclear program, NASA and other US agencies using only a Commodore Amiga personal computer and a "blue boxing" program found online. In 1995, Russian software engineer Vladimir Levin hacks into Citibank's New York IT system from his apartment in Saint Petersburg and authorizes a series of fraudulent transactions, eventually wiring an estimated $10 million to accounts worldwide. The case of Kevin Mitnick was also an important event that year. Mitnick at the end of his supervised release hacked into Pacific Bell voice mail computers. He intercepted and stole computer passwords, broke into private e-mails and altered computer networks. He was finally arrested after a very public pursuit. He got a sentence of 68 months in jail and after serving five years he was released. There was also supervised release for three years and he was prohibited from profiting from films or books that were based on his criminal activity for a duration of seven years. (Mitnick Security, n.d.)

In cases involving cyber-crimes it tends to be people that have limited knowledge on how computer systems work that run the risk of being the main victims of cyber-criminals. The members of the younger generations were practically raised on technology, so they have more technological knowledge while the older people tend to be victims often. There must be better protection measures in place to protect people against cyber-crimes. Cyber-crimes cause businesses to suffer losses in a scenario where hackers steal valuable and confidential information from a company. The information could include the plans of the company, which the hacker could sell to competitors of that company and in this way, set the company back so many steps (Bassett, J., and Evergreen, N., pg. 02). In a different scenario, the company ends up wasting so much time handling the harmful incidents caused by Cyber-crimes. The wasted time reduces the productivity of the enterprise. Many companies also spend a lot of time creating preventive measures. The energy put in investing in this preventive measure is also a derailleur and is one of the impacts of cybercrime. Cyber-crime could cause people to lose confidence in a company. For instance, people would not feel safe banking or involve themselves with a hacked organization. They would feel insecure about sharing their confidential information with such an organization. This aspect affects the productivity of the team (Seger, 121). Further, the rising costs of stopping viruses and malware affects the companies financially. Cyber-crimes cause a lot of harm and frustration especially in a scenario where the individual has no knowledge of the offense. Some of the current cyber criminals are so bright that they could hack and steal information without leaving the slightest clue. Using the

information for the evil purposes eventually affects the individual in an adverse way, leaving them feeling extremely frustrated. The fact that there are few tangible ways of recovering the lost money or information makes it even worse because the individual finds himself in a situation where there is nothing, they can do about the situation

People could prevent cyber-crime in various ways. Knowing the location of all the software that a person uses would reduce the cases of software vulnerability and its usability. In other cases, people try to learn to people's passwords through observation. In this case, people must be aware of their surroundings, type fast and ensure that people do not have the chance of observing their passwords. Another good prevention method is ensuring that the firewall always remains on (Cukier, Wendy, and Levin, 278). An upgrade or replacement would provide even better security. Installation of windows updates would reduce any Windows vulnerability. In a case of weak configurations, the individual could get professionals. The use of spam blockers would help the users end the issue of receiving bogus mail. Most internet providers provide a blocking feature that helps stop fraudulent and phishing emails. On the topic of anti-virus, the individual must ensure that they update it regularly and scan the computer often to remove any malware on the computer. There are free versions available but for better security an individual must consider investing in the best options available. Users with children should ensure that they have parental control software which helps limit the children's whereabouts online. This issue is the wise thing to do because at times the children to go online and check malicious sites without knowing. The parent could monitor the websites that the child visits as one of the ways of spending more time with their children. Ensuring that the mother keeps the firewall on is also vital in ensuring that they keep hackers from accessing the computer. An excellent way to the creation of robust passwords those are hard to compromise (Scutt, 303). Another good idea on the issue of passwords is the use of random passwords. Constantly changing the password also helps the person stay ahead of any hackers. On the issue of malware, individuals must ensure that they use the lasts anti-viruses and anti-spy software that prevent and kill off any malware. In the case of misplaced gadgets, the person should make sure they have passwords securing their systems.

The enforcement of proper intellectual property act laws could further enhance the reduction of cyber-crime. The crime of equipment an intellectual property section has the role of implementing national strategies that help in intellectual properties crimes and cyber-crimes from all around the world. Comprehensive programs like the cyber-crime initiative have the task of creating programs designed to help deal with data thefts, electronic penetrations, and cyber-attacks that occur on crucial information. The section has a role in investigating, preventing and prosecuting cyber-crimes. Working with government agencies, academic institution, the rivet sector and foreign counterparts could help the section deal with cyber-crimes. Law enforcers should be required to invest more time in training in this field. They also must specialize and learn more about technology and all its technicalities. This would help officials understand the maneuvers that can be used in hacking and how to notice the different methods that fit the criteria and how to deal with them. Using the people caught as part of community service could help in dealing with the issue of cyber-crimes. Big business and individuals should further ensure that they have the latest security measure on a regular basis to avoid creating any vulnerability to their businesses.

Various terms are used to define the activities that occur in cyber-crime. Fraud involves illegally taking money from individuals through tricking them. Fraudulent people are the highest population that are involved in cyber-crimes. Fraudsters have various ways of attaining their

goals. Emails from prominent organizations or individuals are used by cyber-criminals to lure innocent people to share amounts of money or information for non-existent products and services. The most nefarious is the hiring of a hacker. Hackers are divided into two groups: white hat and black hat hackers. White hat hackers are hired by organizations and companies to test their security systems and note any flaws that could be exploited to that they can be dealt with. Black hat hackers are a different breed. According to Kaspersky (a company well versed in cyber-security), “Black Hat hackers are criminals who break into computer networks with malicious intent. These types of criminals are the villains of the computer world because they infiltrate and damage both networks and computers for their own purposes. Identity theft is another form of cyber-crime that has seen a prominent rise in recent times. It involves the use of another person's identity illegally. This aspect means that the individual has no knowledge of the use of his character and their personal information is used to commit crimes which can affect their livelihood.

Today, people use computers for many different reasons depending on their level of skill and their needs. A look at the number of people using computers today reveals a surprisingly high number of individuals. This means that adequate measures must be taken to curb the rising trend that is cyber-crime.

References

1. The Council of Economic Advisers. (2018). “The Cost of Malicious Cyber Activity to the U.S. Economy.” Retrieved from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
2. Herjavec R. (2019) “Cybersecurity CEO: The History Of Cybercrime, From 1834 To Present” Retrieved from https://www.herjavecgroup.com/history-of-cybercrime/
3. Mitnick Security. (n.d.). “About Kevin Mitnick” Retrieved from https://www.mitnicksecurity.com/about/kevin-mitnick-worlds-most-famous-hacker-biography
4. Who is Kevin Mitnick? (n.d.) Retrieved from https://www.knowbe4.com/products/who-is-kevin-mitnick/
5. Bassett, J. and Evergreen, N. 'Shirley Homes and the Cyber Thief.' (2008).
6. Seger, Alexander. 'Cyber Crime and Economic Crime.' Financial Crimes: A Threat to Global Security. (2012): pp119-146.
7. Cukier, Wendy, and Aver Levin. 'Internet Fraud and Cyber Crime.' Crimes of the Internet. (2009): pp251-279.
8. Kaspersky. “What is a Black Hat Hacker” Retrieved from https://www.kaspersky.com/resource-center/threats/black-hat-hacker