AN ANALYSIS OF CYBERCRIME

Mahalakshmi Vaishnabi, Royal Global University

INTRODUCTION

Cybercrimes, often known as computer crimes, involve the use of a computer as a tool to further illicit objectives like fraud, identity theft, etc. Most cybercrimes are committed to benefit the perpetrators generally, however some are committed to render targets inoperable. The persons who commit cybercrimes are known as cybercriminals.

CYBERCRIME

The term "cybercrime" is used to denote a broad variety of illegal behaviours carried out on computers or computer networks as a tool, target, or area of crime. This covers everything from electronics cracking to denial service attacks. It is also applied to more conventional crimes where the illicit acts are made possible by networks or computers.

Cybercrime is predicated on state punishment and, like traditional crime, is an act or omission that results in the breaking of the law. Cybercrime is made up of two key components: mens rea and actus reus. The biggest factor contributing to the risk of cybercrime is how strongly dependent we have become on computers and the internet. There are certain activities that put the country's laws, government, and security in danger.

Particularly with credit card and payment schemes, cyber assaults or crimes have seriously harmed commercial banks' data. Because of the close ties between market infrastructure and digital systems, cybercrime is rampant. The size and use of the account contribute significantly to the losses brought on by online fraud in the retail sector, but the damage that may be done by an online attack on financial infrastructure is limitless. Markets also react to fresh information from online data storage as well as traditional social media like newspapers and youth media like social media. Therefore, another method online cybercrime could harm markets is through actual change and the dissemination of false information.

With the formation of intermediate partners a small number of institutions indirectly exposes the entire financial industry to computer risk, with unintended and poorly understood results.[1]

HISTORY OF CYBER CRIME

1834 - French Telegraph System - A group of thieves robs the French Telegraph System and steals financial market data, successfully operating the world's first cyber attack.

1870 - Switchboard Hack - A young man employed as a switchboard operator was able to disconnect and redirect calls and use the line to operate himself.

1878 - Early Calling - Two years after Alexander Graham Bell set up the phone, Bell Telephone Company fired a group of teenage boys from the New York telephone system for repeatedly and deliberately misleading and cutting off customer calls.

1903 - Wireless Telegraphy - When John Ambrose Fleming publicly unveils Marconi's "secure" phone technology, Nevil Maskelyne interrupts him by sending malicious code messages insulting the establishment.

1939 - Military Codebreaking - Alan Turing and Gordon Welchman built BOMBE, an electro-mechanical machine, during WWII while working as codebreakers at Bletchley Park.

1940 - First Ethical Hacker - Rene Carmille, a member of the Nazi-occupied Resistance in France and a computer punch-card specialist who owned equipment used by the Vichy government in France to process information, discovered that the Nazis used punch-card machines to process and track Jews, volunteers allowed them to use their own, and then collected it to thwart their plan.

1957 - Joybubbles - Joe Engressia (Joybubbles), a blind, seven-year-old boy with the right voice, hears a high-pitched phone call and begins to whistle at 2600Hz, which enabled him to communicate with the phone lines and was the first US phone shooter or "phone phreak."

1962 - Allan Scherr - MIT establishes first computer names, student privacy and time limits. Student Allan Scherr made a punch card to trick the computer into printing all the passwords and using them to log in like other people after the end of his term. He also shared passwords

[1] Frunza, Marius-Christian, *Introduction to the Theories and Varieties of Modern Crime in Financial Markets*, 2016 Cyber Crime, Science Direct, https://www.sciencedirect.com/topics/computer-science/cybercrime (accessed on 28th March 2022)

with his friends, leading to the first "troll" of the computer. They log into their teacher's account and leave funny messages about him.

1969 - RABBITS Virus - A stranger installed a program on a computer at the University of Washington Computer Center. An invisible system made its own copies (breeding like a rabbit) until the computer overloads and stops working.

1970-1995 - Kevin Mitnick - Since 1970, Kevin Mitnick has been infiltrating some of the world's most watched networks, including Nokia and Motorola, using social engineering schemes, tricking insiders into giving out codes and passwords, and using codes. access to internal computer systems. He became the most wanted cyber criminal at the time.

1971 - Steve Wozniak and Steve Jobs - As Steve Wozniak reads an article about Joybubbles and other telemarketing, he becomes acquainted with the John "Captain Crunch" Draper and learns to hack telephone systems. He built a green box designed to hack phone systems, even pretending to be Henry Kissinger and performing tricks that cost the Pope. He began the mass production of the machine with his friend Steve Jobs and sells it to his classmates.

1973 - Fraud - A New York local bank merchant uses a computer to defraud more than $ 2 million.

1981 - Cybercrime Conviction - Ian Murphy, nicknamed "Captain Zap," hacked the AT&T network and changed its internal clock to charge high operating costs over peak hours. The first person convicted of cybercrime, and the inspiration for the film "Sneakers," did 1,000 hours of community service and 2.5 years of probation.

1982 - Logic Bomb - The CIA detonated a Siberian Gas pipeline without the use of a bomb or an arrow by coding the network and the computer system that controlled the gas pipeline. The code was embedded in machines purchased by the Soviet Union from a Canadian company.

1984 - US Secret Service - U.S. Comprehensive Crime Control Act gives the Secret Service the power to control over computer fraud.

1988 - The Morris Worm - Robert Morris created what was to be known as the first worm on the Internet. The worm is removed from a computer at MIT to suggest that the creator was a student there. Possibly harmless exercise soon became a vicious denial of a service attack when

an insect on the way to spread the worm led to computer infections and re-infected at a faster rate than expected.

1988-1991 - Kevin Poulsen - In 1988, unpaid debt in storage led to the discovery of empty birth certificates, fake IDs, and a photograph of criminal Kevin Poulsen, known as "Dark Dante," breaking into a telephone company car. In connection with a nationwide search campaign, he continued to rob, including robbing the Los Angeles radio station's telephone wires to make sure he was the right caller in a charity contest.

1989 - Trojan Horse Software - Diskette claiming to be a source of information about AIDS was sent to thousands of AIDS researchers and subscribers to the UK online journal. Contains a Trojan (after Trojan Horse of Greek mythology), or malicious program.

1994 - Datastream Cowboy and Kuji - Managers at Rome Air Development Center, a U.S. research center. Air Force, they found the password "sniffer" installed on their network, endangering more than 100 user accounts. Investigators have found that two hijackers, known as Datastream Cowboy and Kuji, were the attackers.

IMPACT OF CYBERCRIME

Technological innovations that changed how people communicate and interact during the 21st century. A worldwide digital era is responsible for the social, political, and economic aspects of human life. The use of computers and other electronic devices has generally grown quickly. A major rise in crime has resulted from these changes, particularly online. As hackers create new and sophisticated techniques every day, cybercrime has increased rapidly. The global pace of cybercrime growth is frightening, despite the efforts made by the international community to stop this cycle of violence and lessen its effects.[2]

A company or individual may be the target of a harmful cyberattack. Every piece of information is now used on computers because we live in a technologically advanced age. Attacks on computers and other electronic equipment are considered cybercrime. The organisation and the nation as a whole could both be in peril from this cyberattack. Numerous instances of digital attacks have occurred in India and other countries to date, necessitating increased security

[2] Alghamdi I. Mohammed, *A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide*, [Volume 09,] [Issue 06 (June 2020)] INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) ,https://www.ijert.org/a-descriptive-study-on-the-impact-of-cybercrime-and-possible-measures-to-curtail-its-spread-worldwide

precautions. If not initially contained, these attacks—which also include fraud, malware, cyberstalking, and other things—have an impact on the nation's economy. As a result, businesses and government organisations are actively spending in the upkeep and employment of specialists in computer crime.

However, now the most sophisticated cybercrime network operates to attack the system for data collection. Three types of cybercrimes- Against the Individual, against the Property, against the Government.

Law enforcement agencies have taken this type of cybercrime seriously over the years. It now keeps track of all individual attacks of this type. In a cyber world, invaders steal data, similar to how criminals steal property in the real world. The attacker steals someone's banking information and uses the credit card to make online purchases. The attacker attacks the site with malicious software in order to disrupt the organization's system. Cyber terrorism refers to these types of crimes. This is concerning because the attacker may discover sensitive documents related to government projects. Such attacks are frequently carried out by an enemy nation or terrorist group. Terrorists have stolen government data in numerous cases around the world..

Such attacks are frequently carried out by an enemy nation or terrorist group. Terrorists have stolen government data in numerous cases around the world. Furthermore, financial crime occurs when a criminal steals money from a user account holder. Furthermore, they steal the company's data as well as its finances. Robbery is a punishable offence in many countries, including India. It is not the same as moral theft. Various types of software are used in a typical hijacking to infiltrate a targeted system. The hacker can then track everything a person does to commit theft. Many movies in India were filmed on download sites before they were released, resulting in copyright infringement.

In other words, theft is also known as privacy, and it causes significant harm to an organisation. In India, there are many cases of cyber stalking, which sometimes leads to the victim committing suicide. This is a system hacker and a targeted data victim. Many laws have been enacted in India to combat this threat. It can be personal or organisational; these laws help reduce or eliminate the number of cases of digital crimes.

The Impact of Cyber Crime on Socio-Eco-Political Riders

In other words, theft is also known as privacy, and it costs a company a lot of money. In India, there are frequent instances of cyberstalking, which occasionally leads to the victim committing suicide. This is a victim of targeted data and a system hacker. Numerous laws have been passed in India to address this problem. These regulations aid in the decrease or eradication of these digital crimes, whether they be personal or organisational.

Additionally, one of the key elements affecting criminal activity is the population. The rising crime rate and the nation's population have been found to be positively correlated.

Criminal activity is conceptually a dynamic and relative occurrence, as well as relative social, political, and economic changes that take place in already-existing social institutions. As a result, there is never enough time for an exhaustive definition of crime that covers every facet of it and cannot be applied to other civilizations as a whole. The phenomena that occur in the value system created by these changes are associated with dynamic differences. Economic crime is at its peak right now, by the way. This amply demonstrates the interdependence of crime on social and political structures as well as political materials.

In addition, the population is one of the important factors that affect crime cases. There is a positive correlation between crime cases and the growth of the national population. In addition to the population, the situation of a specific place,migration of the population of the population of the population of the neighborhood, the emigration of the income of the income, etc.[3]

Since all crime control programs are closely related to the political system it claims procedures, making laws, creating a measure of prevention, political structure and system also have an impact crime in a particular community. This clearly shows that every definition of crime has something to do with it socio-economic factors.

Youth and Cybercrime: Its Effects

The biggest worry among young people today is cyberbullying. Since five years ago, it has become widespread; typically, starting at the age of 18, they may be easily reached and frightened in cyberbullying. It has turned into a frightening practise in our society. Terrible

[3] Rao Yerra Shankar, Pradhan Debasish, Panda Tarini Charana, Rath Ranjita, *Digital Crime and its Impact in Present Society* NCRTAPSE – 2020 (Volume 8 – Issue 01) (published on 08-02-2020), IJERT https://www.ijert.org/digital-crime-and-its-impact-in-present-society

remarks, unpleasant images, or negative comments from another individual constitute cyberbullying, which is akin to a panic attack.

Pornography

Pornographers offer their material to interested parties and sex addicts online. In India, it is against the law to watch and keep this kind of material. In today's society, pornography has taken on a business-like quality as people partake in it in order to profit financially.

They even install covert cameras, violating people's right to privacy in places like hotels, hostels, and changing areas in shopping centres, among others.[4]

The use of cyberspace to publish, distribute, or design pornography is referred to as cyber pornography. Technology has advantages and disadvantages, and cyber pornography is a result of technological advancement. People can now view thousands of pornographic videos on their mobile phones or laptops, and they can even upload pornographic content to the Internet. [5]

CONCLUSION

Crime affects everyone and in the future cybercrime will affect more people irrespective whether the people are rich or poor. [6]

Cyber crime is not something that can happen in the future. It is done every day right now. Thieves commit cybercrime to steal people's money and identity. A virus can destroy someone's files and a lost website can lead to the acquisition of unwanted commercial calls.

Cybercrime is already a major problem worldwide, and it is growing rapidly. The legal world is trying to catch up; legislatures are enacting new laws to deal with this new form of crime, and police stations are setting up specialized computer crime centers and pressuring their officers to become more technologically savvy.[7]

---

[4] *Pornography As Cyber Crime*, https://www.legalserviceindia.com/legal/article-914-pornography-as-cyber-crime.html (accessed on 1st march 2022)

[5] Chiildar Nidhi, *Cyber Pornography*, Ipleaders,(July 9 2019), https://blog.ipleaders.in/cyber-pornography/ (accessd on 1st march 2022)

[6] Giles John, (May 29th 2021), *Cybercrime affects everyone* , Michalsons, https://www.michalsons.com/blog/cyber-crime-and-cyber-security-affects-everyone/18167 (accessed on 1 st march 2022)

[7] Ibid Page ,*Facing the Cybercrime Problem Head-On* , Shinder Littlejohn, Cross Michael , in Scene of the Cybercrime (Second Edition), 2008 (28th february 2022)

Cybercrime, like most crimes, is a public and legal problem. To combat it effectively, involvement of exerts in the IT community (many of whom may be reluctant to participate) as well as those in the community affected by, directly or indirectly, are essential to tackle down the criminal act that has been found in a virtual environment .

Cybercrime is one of the crimes against which it is committed an online or electronic site for its own purpose.

REFERENCES

Websites:-

Frunza, Marius-Christian, *Introduction to the Theories and Varieties of Modern Crime in Financial Markets*, 2016 Cyber Crime, Science Direct, https://www.sciencedirect.com/topics/computer-science/cybercrime (accessed on 28th March 2022)

Herjavec Group , August 26, 2021, *Cyber CEO: The History Of Cybercrime, From 1834 To Present*, https://www.herjavecgroup.com/history-of-cybercrime/ (accessed on 28th February 2022)

Chiildar Nidhi, *Cyber Pornography*, Ipleaders,(July 9 2019), https://blog.ipleaders.in/cyber-pornography/ (accessd on 1st march 2022)

Giles John, (May 29th 2021), *Cybercrime affects everyone* , Michalsons, https://www.michalsons.com/blog/cyber-crime-and-cyber-security-affects-everyone/18167 (accessed on 1 st march 2022)

Giles John, (May 29th 2021), *Cybercrime affects everyone* , Michalsons, https://www.michalsons.com/blog/cyber-crime-and-cyber-security-affects-everyone/18167 (accessed on 1 st march 2022)

Alghamdi I. Mohammed, *A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide*, [Volume 09,] [Issue 06 (June 2020)] INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) ,https://www.ijert.org/a-descriptive-study-on-the-impact-of-cybercrime-and-possible-measures-to-curtail-its-spread-worldwide

Herjavec Group , August 26, 2021, *Cyber CEO: The History Of Cybercrime, From 1834 To Present*, https://www.herjavecgroup.com/history-of-cybercrime/ (accessed on 28th February 2022)

Frunza, Marius-Christian, *Introduction to the Theories and Varieties of Modern Crime in Financial Markets*, 2016 Cyber Crime, Science Direct,

https://www.sciencedirect.com/topics/computer-science/cybercrime (accessed on 28th March 2022)