LEX SCRIPTA MAGAZINE OF LAW AND POLICY

ISSN- 2583-8725

VOLUME-1 ISSUE-1
YEAR: 2023

EDITED BY:

LEX SCRIPTA MAGAZINE OF LAW AND POLICY

LEX SCRIPTA MAGAZINE OF LAW AND POLICY, VOLUME-1: ISSUE-2

LEX SCRIPTA MAGAZINE OF LAW AND POLICY, VOL-1, ISSUE-1
ISSN-2583-8725

CYBERSECURITY: CATEGORIES AND CHALLENGES

AUTHOR: ISHAN KRISHNAN

ABSTRACT

The importance of cyber security is growing for people, businesses, and governments across the globe. One of the biggest issues in cybersecurity is keeping our data safe in a world where everything is online, from cute kitten videos and our vacation journals to our credit card information. There are many different types of cyber security concerns, including ransomware, phishing, malware assaults, and more. In terms of local cyberattacks, India is ranked 11th worldwide and has already had 2,299,682 occurrences in the first quarter of 2020.

Digital technology is encompassing all occupations, all over the world and has brought the real meaning of globalization. At one end the digital technology or the cyber system has provided opportunities to communicate around the world and on the other end some individuals exploit this opportunity for criminal practices. Criminals take advantage of the internet and other global network connections to exploit online sources. The situation is alarming. Cybercrime is the talk of town in every sphere. Everyday a new technology is being developed for committing cybercrime and often to tackle new cybercrimes lack of proper backup technology is observed. Therefore, the cybercrime investigation becomes difficult without proper framework. The primary objective of this paper is to categories cybercrimes or e-crimes, challenges faced and how to manage it.

Keywords – cybercrime, digital technology, internet, cyber system, e-crimes.

INTRODUCTION

Like every other area of life, technology offers advantages and disadvantages. The quality of a person' s life is improved in practically every area, including health care, transportation, communication, smart cities, etc. We must overcome a number of obstacles if we want to avoid making technology our own worst enemy.

More than any other area of technology, cyber security is a danger. Technology-controlled gadgets are already being abused by cybercriminals to further crimes like theft and fraud. It is exceedingly challenging to prevent such cyber-attacks using technological standards that are still under development and improving gradually. The evolution of technology and increasing accessibility of smart tech means there are multiple access points within users' homes for hackers to exploit. While law enforcement attempts to tackle the growing issue, criminal numbers continue to grow, taking advantage of the anonymity of the internet.

As more people connect to the digital world, cybercrime is expanding at a similar rate. Cybercrime may be said to be those species of which the genus is the conventional crime and where either a computer is an object or subject of the conduct constituting a crime or any criminal activity that uses a computer either as an instrumentality, target, or a means for perpetuating further crimes. In the present situation, e-crime has been one of the major concerns as it has been increasing rapidly. Cybercrime occurs in a wide range. Thus,

WHAT IS CYBERCRIME?

When early computerized phones became a target in the 1970s, cybercrime history began. Through a set of codes, tech-savvy individuals discovered a technique to avoid paying for long-distance calls.

They were the earliest known hackers to manipulate hardware and software to steal long-distance phone time.

People became aware of the vulnerability of computers and other digital devices as a result of this. Major risks are now being created for individuals who are online. The economies of numerous countries have been severely impacted. Additionally, as technology advances, implications are growing quickly. As a result, fighting cybercrime is turning into an extremely challenging endeavor for law enforcement agencies.

A definition can be yielded that any unlawful acts wherein the computer is either used as a tool or as a target for committing crime, is cybercrime.[1]

Cybercriminal is a person who commits an illegal act with a guilty intention with respect to the cyber system. Such criminals can be hackers, organized hackers, or cyber terrorists. E-crime can include any range of unlawful activity, such as, money laundering, intellectual property, economic espionage, online extortion, pornography, or non-delivery of any product purchased online. It is not easy to identify crime methods.

Following is a list of *cyber criminals*:

i. Crackers – individuals who intend to cause loss to satisfy antisocial motives. Virus creators and distributors also fall into this category.

ii. Hackers – individuals who explore others' computer systems.

iii. Pranksters – individuals who perpetrate tricks on others. Generally, they do not intend any harm.

iv. Career criminals – individuals who earn most of their income from e-crimes. Their contents are usually malicious.

v. Cyber terrorists – they can be of several types. They are individuals who break into government websites or websites of any other leading organizations. They can also be a group of individuals who crash a website by flooding it with traffic.

vi. Cyber bulls (cyberbullying) – any harassment that occurs via the internet. Name-calling in chatrooms, malicious emails, posting fake profiles are some of the cyber bullying.

vii. Salami attackers – individuals who make alterations in financial institutions which are completely unnoticed. For example, an employee of a bank inserts some program that would deduct an exceedingly small amount from accounts of all the customers.

Modus operandi, when, where, and by whom the crime was committed gets difficult to investigate as the algorithm of the internet gives a perfect platform for any criminal activity.

REASON FOR COMMITTING E-CRIME

Cybercriminals always opt for an easy way to make a huge profit. They target people or organizations who are rich, where huge amounts of money flow on a daily basis and can be hacked easily.

[1] *Security, Panda Security P. (2021b, April 26). Types of Cybercrime. https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/ Mediacenter.*

Some of the e-criminals do it for the sake of recognition or to fight for a cause which he thinks is correct and attract masses to conduct any kind of antisocial movements. Low marginal cost of online activity due to global reach makes it effortless for criminals to hack into systems. Official investigation takes a comparatively longer period of time since evidence can be deleted and retrieval of data is tough. Lack of reporting standards and difficulty in identification of type crime makes it troublesome for criminals to do their work. Codes, intellectual property, high profiled data, and other information are sold at a very pricey range, giving them an opportunity to make money really quickly.

CAUSES OF CYBERCRIME

Number of cybercrimes are increasing across the globe. Computers are vulnerable, so laws are required to protect and safeguard them against cybercriminals.[2] Due to the complex technology, the computer can be breached. Hackers can steal access codes, fingerprints, retina scans etc. that can easily be used to fool biometric systems and bypass firewalls can be utilized to get past many security systems.[3] Data may be stored on the computer in an unusually minimal amount of space. This makes it much easier for individuals to steal data from other storage systems and exploit it for their own financial gain.

Cybercriminals take advantage of the gaps created by imperfect program codes. Negligence is another cause of malware interference. Data erasing is one of the biggest causes of e-crime. Data related to crime can be destroyed and no traces may be found, paralyzing the whole investigation.

CATEGORIES OF CYBERCRIME

Cybercrimes are broadly classified into three:

i. **Crime Against Individuals**

Cyber Defamation, hacking, indecent exposure, spoofing emails, IRC crime (Internet Relay Chat), net extortion, malicious code, trafficking, distribution, posting, phishing, credit card fraud, and the dissemination of pornographic material, including software piracy, are all examples of cybercrimes committed against individuals. The potential harm of such a crime to an individual person can hardly be bigger.

ii. **Crime Against Property**

e-crime against all forms of property. These offences include salami attacks, intellectual property crimes, and computer vandalism (erasing other people's property). This type of crime is frequently committed at financial institutions or with the intent to conduct financial crimes.

This sort of offence has a crucial characteristic in that the alteration is so minute that it would typically go unnoticed.

---

[2] *Bandakkanavar, R. (2022, June 27). Causes of CyberCrime and Preventive Measures https://krazytech.com/technical-papers/cyber-crime*

Bandakkanavar, R. (2022, June 27). Causes of CyberCrime and Preventive Measures https://krazytech.com/technical-papers/cyber-crime

Krazytech.

[3] *Krazytech.*

iii. Crime Against Organization

One specific type is cyberterrorism. The advancement of the internet has shown how individuals and organizations are using the standard of cyberspace to intimidate national and international governments as well as to terrorize their citizens. When a person cracks into a website that is administered by the government or the military, this offence clearly becomes terrorism.

MEASURES AGAINST CYBERCRIME

To tackle cybercrime effectively, establish multidimensional public-private collaborations between law enforcement agencies, the information technology industry, information security organizations, internet companies, and financial institutions. Unlike the real world, Cybercriminals do not fight one another for supremacy or control.[4] Instead, they cooperate to enhance their skills and even support one another in finding new possibilities. Therefore, the traditional means of criminal justice cannot be applied to cybercriminals. Utilizing the solutions offered by Cross-Domain Solutions is the best course of action. This enables companies to employ a single system made up of both software and hardware to authenticate information access and transfer when it occurs between multiple security classification levels. This enables smooth information sharing and access inside a certain security classification but prevents information from being intercepted or accidentally released to users outside of that security classification. This promotes the security of the network and the systems connected to it.

By maintaining strong passwords, being social media savvy, using trusted sources to download or to surf through the internet are some other measures.

Data encryption can be used to secure sensitive data. Keeping the computer system linked with latest patches and updates along with strong security software.

In the case of children using the technology, **parent control** should be enabled. children‘ s computer systems should be checked frequently to safeguard them from any kind of crime.

CYBER LAWS IN INDIA

India's cyber laws have aided in the growth of electronic commerce and government by ensuring maximum connection and reducing security concerns. Additionally, this has increased the breadth and efficiency of digital media and made it available in a larger range of applications.[5]

- **Information Technology Act, 2000 (IT Act)**

IT Act, 2000 is the first cyberlaw approved by the Indian Parliament. The Act defines its object as following:

"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker"s Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."[6]

---

[4] *Bandakkanavar, R. (2022, June 27). Causes of CyberCrime and Preventive Measures. Krazytech. https://krazytech.com/technical-papers/cyber-crime*

[5] *Garg, R. (2022, April 28). Cybercrime laws in India. iPleaders. https://blog.ipleaders.in/cyber-crime-laws-inindia/*

[6] *Garg, R. (2022, April 28). Cybercrime laws in India. iPleaders. https://blog.ipleaders.in/cyber-crime-laws-inindia/*

Following are the sections that directs the process to investigate cybercrimes:

i. Section 43 - pertains to those who engage in cybercrime, such as harming the victim's computer without the victim's proper consent. If a computer is damaged in such a case without the owner's permission, the owner is completely entitled to a reimbursement for the whole damage.

ii. Section 66 - applies to any dishonest or fraudulent conduct covered. In such cases, the maximum penalty is three years of imprisonment or a fine of Rs. 5 lakhs.

In *Poona Auto Ancillaries Pvt. Ltd., Pune v. Punjab National Bank, HO New Delhi & Others (2018),* Rajesh Aggarwal of Maharashtra's IT department (representative in the present case) ordered Punjab National Bank to pay Rs 45 lakh to Manmohan Singh Mattharu, MD of Pune-based firm Poona Auto Ancillaries. In this case, a fraudster transferred Rs 80.10 lakh from Matharu's account at PNB, Pune after the latter answered a phishing email. Since the complainant responded to the phishing mail, the complainant was asked to share the liability. However, the bank was found negligent because there were no security checks conducted against fraudulent accounts opened to defraud the Complainant.

iii. Section 66 B to 66 F – describes the penalties for fraudulently receiving stolen communication devices or computers; digital signatures, password hacking, other forms of identity theft; cheating by personation using computer resources; taking pictures of private areas, publishing or transmitting them without person' s consent; cyber terrorism respectively with respective punishments of fine and imprisonment.

iv. Section 67 - involves electronically publishing obscenities. If convicted, the prison term is up to five years and the fine is up to Rs 10 lakh.

➢ **Indian Penal Code, 1860 (IPC)**

If IT Act does not cover sufficient crimes, following IPC sections would be applicable:

i. Section 292 - Although the initial aim of this section was to address the selling of pornographic materials, it has now developed to cover a variety of cyber offences as well. This clause also applies to how pornographic or sexually explicit activities of children are publicized or distributed electronically. Such offences are punishable by up to two years in jail and penalties of Rs. 2000. For repeat (second time) offenders, any of the aforementioned offences may result in a sentence of up to five years in jail and a fine of up to Rs. 5000.

ii. Section 354 C - According to this section, cybercrime is defined as the taking or publication of images of a woman's privates or intimate acts without her consent. Voyeurism is the only topic covered in this section because it is illegal to observe a woman engage in sexual activity. Sections 292 of the IPC and Section 66E of the IT Act are wide enough to cover offences of a similar character in the absence of this section's essential components. First-time offenders may receive a sentence of up to three years in jail, while repeat offenders may receive a sentence of up to seven years.

iii. Section 354 D – This section describes and penalizes stalking, including both physical and online stalking. Cyberstalking is the practice of tracking a woman through technology, such as the internet or email, or contacting her despite her lack of interest. For the first offence, this crime has a maximum sentence of 3 years in jail; for the second offence, it carries a maximum sentence of 5 years in prison and a fine.

A victim in the case *Kalandi Charan Lenka v. the State of Odisha(2017)* has received a series of obscene messages from an unknown number that has damaged her reputation. The accused also sent emails to the victim and created a fake account on Facebook containing morphed images of her. The High Court,

therefore, found the accused prima facie guilty of cyberstalking on various charges under the IT Act and Section 354D of IPC.

iv. Other sections, Sections 379, 420, 463, 465 and 468 also deal with certain provisions related to cybercrime.

CONCLUSION

Cybercrime has created a major threat to those who use the internet, with millions of users' information stolen within the past few years. It has also made a major dent in many nations' economies. IBM president and CEO Ginni Rometty described cybercrime as ―the greatest threat to every profession, every industry, every company in the world.‖ Read below for shocking statistics on cybercrime's impact on our society to date.

Technology development has led to the emergence of unpleasant aspects on the dark web. Intelligent individuals have turned the Internet into a tool for immoral activities, which they frequently use for financial benefit. Cyber laws therefore enter the picture at this time and are crucial for every person. Some actions are categorized as grey activities that are not subject to legal regulation since cyberspace is an incredibly challenging area to manage. Because the cyber criminals sit in one nation and access the computer from another, we are aware that it might be challenging to detect these hackers. The best way to prevent this is for us to be watchful and vigilant, and to always use strong and unique IDs and passwords online.