Original Article

A Case Study on Defending against Cyber Crimes

Amrita Sen[1], Gunamani Jena[2], Subhashree Jena[3], Dr P Devabalan[4]

[1] Ph D scholar CMJ.

[2] Professor CSE.

[3]Ph D scholar, Annamalai University.

[4] Professor, CSE BVC.

Email: amritasengupta.edu@gmail.com[1], drgjena@gmail.com[2], sjena96@gmail.com[3], devabalanme@gmail.com[4]

DOI: 10.47750/pnr.2022.13.S01.229

Abstract

Cyber terrorism is the premeditated, politically motivated assault on information, computer systems, computer programmes, and data that results in violence against property, the government, and the general populace. In the age of globalisation, the use of steganography as a form of internet terrorist communication – Red Fort case, E-mail threats in Taj Mahal case, and Supreme Court E-mail Threat case. The use of the internet by terrorists to organise and execute the September 11 World Trade Centre attack reflects the current state of affairs and provides the answer to the question, "Is the internet the new boon or bane of science?"In India, cyber laws prohibit any crime committed with the aid of technology, where a computer is a tool for cybercrime. Cybercrime rules prevent citizens from sharing sensitive information with strangers online. Since the establishment of cyber laws in India, the IT Act 2000 was enacted in 2000 and updated in 2008 to cover all sorts of cyber offences in India. Without a doubt, India's Cyber security or Cyber laws give protection against cybercrime. However, prevention is always preferable to treatment.Cyber law and cyber crimes have also become more complicated in today's technologically advanced society. Internet and technology were developed for research purposes and to make human life easier, but as the number of people using the internet in India expanded, the necessity for Cyber Laws became apparent. Due to the anonymous nature of the internet, it is simple to commit cybercrimes. Consequently, numerous individuals could abuse this component so extensively. Therefore, India has a need for cyber law.

Keywords: Cybercrime, Cyber Law, Steganography, National Cyber Investigative Joint Task Force

INTRODUCTION

Cybercrime, often known as computer-oriented crime, involves a computer and a network. The computer may have been used to commit a crime, or it may be the intended victim. Cybercrimes are defined as: "Offenses committed against individuals or groups of individuals with a criminal intent to intentionally harm the victim's reputation or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern tele communication networks such as the Internet (networks including chat rooms, emails, notice boards, and groups) and mobile phones (Bluetooth/SMS/MMS)" [1]

In 2014, a research (supported by McAfee) projected the annual damage to the world economy to be $445 billion.

In 2012, nearly $1.5 billion was stolen in the United States due to online credit and debit card theft[2]. In 2018, [3]the Centre for Strategic and International Studies (CSIS) and McAfee published a study estimating that around one percent of the global GDP is lost annually to cybercrime, or close to $600 billion.

Each year in India, almost $120 million worth of mobile phones are lost or stolen. Nearly 69% of information thefts are committed by current and former firm workers, whereas only 31% are committed by hackers, according to The Hindu on October 27, 2007. Therefore, if we are technologically competent and use internet banking or online shopping, we need be very cautious about revealing personal information.

• To provide a concise overview of cybercrime and its consequences on the general populace

• The report provides guidelines for defending against cybercrime.

TYPES OF CYBERCRIMES:

Fig.1. Types of Cybercrime

COMPUTER-ASSISTED CRIMINAL ACTIVITY

There are numerous instances of computer-assisted crime in which the computer is used to commit the crime. Several are explored in detail below:

Data Piracy: This relates to the reproduction of digital data and the simple distribution of print, images, sound, and multimedia combinations, as well as the unauthorised use of copyrighted content for personal gain.

Pornography/Child pornography: The unethical and illegal transmission of sexually explicit content that primarily targets minors.

Illegal Interception of Material The increased speed and capacity of data flow over the Internet has increased its susceptibility. Now, it is easier for unauthorised individuals to obtain critical information. It comes in numerous forms, including:

Internet time thefts: Phishing, spoofing, and spam (unsolicited mail), in which a criminal sends phoney e-mails that appear authentic in order to coerce the victim into divulging personal information. [4]

Online Credit Card Fraud, E-Bank Theft: The unauthorised acquisition of a credit card number for online transactions or bank account information in which funds are transferred to a criminally accessible account.

COMPUTER-BASED CYBER CRIMINALITY

There are further instances of Computer Oriented Cyber Crime in which the computer is the target:

The act of obtaining information from a computer storage device or hard drive, as well as stealing a username and password and modifying data, is known as hacking.

This includes document and certificate forgery, identity theft, and counterfeit money.

Changing Websites: In this attack, the hacker modifies the website's messages and deletes or replaces certain pages with new ones that have the same names.

Corporate espionage has become a serious worry for organisations, since approximately 80% of CEOs use detectives and surveillance companies to spy on their ex-workers, employees' lifestyles, and their constant whereabouts, in addition to pre- and post-employment verification.

In addition, as per section 354D, the female ex-employees are permitted to file a FIR, and if the stalking offence is proven, On a first conviction, the offender faces a period of imprisonment of either kind that may last up to three years, as well as a fine. On a second or subsequent conviction, the offender faces a term of imprisonment of either kind that may last up to five years, as well as a fine [5]. It has something to do with e-killing, -homicide, -suicide, or -Spyware [6]

REASONS FOR CYBERCRIME:

Ease of Access: The difficulty in preventing unauthorised access to a computer system is that it is possible to violate the technology by stealing access codes, recorders, PINs, retina imagers, etc., This can deceive several types of security software, including biometric scanners and firewalls.

It is possible for cybercriminals to target specific individuals in order to cause them harm or damage their reputation. It's safe to say this is the most dangerous conceivable explanation. They are committed to the struggle and hope to win. Cyberterrorists is the term used to describe them.

Carelessness It's possible to neglect safeguards in the system. Because of this carelessness, criminals might cause damage to computers.

Revenge, or the desire to hurt one's victim through manipulating a convoluted system, can be seen as motivation or a form of revenge. Those who engage in fraudulent activities through the manipulation of data, such as e-commerce, e-banking, or other forms of electronic commerce, are often young people or those motivated by a desire for quick cash.

Weak Law Enforcement Agencies:

Due to the absence of cyber laws in many nations, numerous cybercriminals escape punishment.

Cybercrimes Committed for Publicity or Recognition: Typically perpetrated by juveniles who wish to be acknowledged without offending anyone's feelings.

ONLINE CRIME INVESTIGATIONS:

According to research, no law can be properly implemented to eradicate cyber crimes. In 2012, cyber crimes increased by 61%, totaling 2,886, with Maharashtra registering the highest number of incidents. During 2008, 2009, 2010, 2011, and 2012cybercrime-related sections of the Indian Penal Code saw a total of 176, 276, 356, 422, and 601 cases reported between 2013 and 2017 (IPC). The previous year exemplified how rapidly the threat landscape continues to grow, as the danger to organisations continues to intensify and now spreads across varied mobile platforms. The Web sense Security Lab reaffirmed that conventional security methods are ineffective against cyber threats. The providers of security must move toward more viable defences. Case studies are presented to expound on the threats and defence strategies against cyber attacks.

Case 1: Examination of Phishing

One Doctor from Gujarat had filed a criminal complaint alleging that certain individuals ("Perpetrators") had committed

fraudulent acts using emails that appeared to originate from ICICI Bank's email address. These actions were committed with the goal to deceive the Customers. The investigation was conducted with the aid of the customer's e-mail, bank account IP details, and domain IP information, and the crime scene was inspected for evidence.

Case 2: Online Credit Fraud and Counterfeiting

One of 2003's most high-profile crimes involved a 21-year-old engineering student named Amit Tiwari who stole more than Rs. 900,000 from CC Avenue, a credit card processing company situated in Mumbai, by using many aliases, bank accounts, and fake customers.

Case 3: Financial Crimes

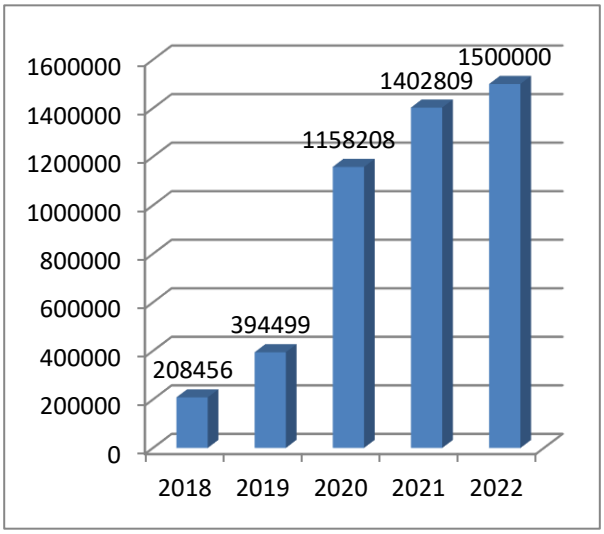
Due to organised criminality, Wipro Spectra mind lost the telemarketing contract with Capital one. In order to increase Capital one's sales, the telemarketing representatives offered bogus discounts and free items to Americans. Surprisingly, the internal audit also discovered that these telemarketers' superiors were complicit in the scheme. [7]

Case 4: Corporate Espionage

In 2013, three individuals stole the customer information of a reputable private insurance firm and utilised it for unfavourable publicity of the company, its policies, and its schemes. These individuals were competitive business owners that engaged in corporate espionage. The theft of client data was a violation of the Information and Technology Act and section 379 of the Indian Penal Code. (Origin: DNA)

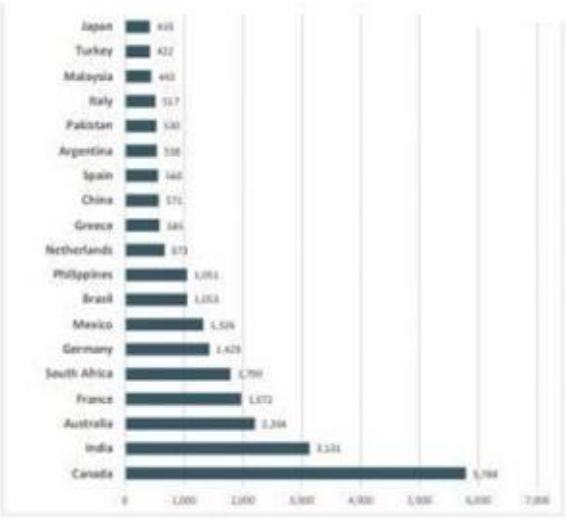
India recorded 2,08,456 cases in 2018, 3,94,499 in 2019, 11,58,208 in 2020, 14,02,801 in 2021, and 2,12,485 in the first two months of 2022.

Fig. 2. Incidents of cybercrime in India



The US Federal Bureau of Investigation (FBI) recently released a report related to the victims of cybercrimes in the world. India ranks **fourth on the list**.

Fig. 3. India's rank world wid



DEFENDING AGAINST CYBER CRIMES:

As demonstrated by the preceding three incidents, established cyber security measures to protect agency networks are essential. Cybercriminals identify security flaws that professional criminals or cyberterrorists may exploit in the future. Securing the connections between government-managed networks and other networks, such as the Internet, is essential for securing and monitoring wireless access points, network access points, and network-connected devices. To prevent insider attacks on agency networks, employees' access to files should be limited to what is strictly necessary for them to do their jobs. Authentication mechanisms for users and hardware should be standardised, as should authentication techniques for users and equipment. 5.3 Networks serving different agencies or departments should be segmented, and access to those segments should be controlled. After the Wipro Spectra mind case, for example, Cyber Crimes and Information Security: Threats and Solutions 839 recommended a thorough security check of all employees, banned the use of mobile phones, and used technology to keep tabs on data logs. 5.5 It was also recommended that all user activity be monitored.

It is important to lock down all hosts that could be DoS (Denial of Service) targets to prevent hackers from gaining access to sensitive data.

Using a Trojan scan tool to ensure a safe installation is a 5.7 must.

To Protect Yourself From Being Exploited: Regularly check for malware such as spyware, adware, and bots (software robots).

Anti-spyware programmes are used to eliminate the threat posed by spyware.

All inbound communications are immediately blocked by the perimeter defence system.

Workers should be given annual security awareness training that includes a warning against downloading software without first obtaining permission from the appropriate authorities.

Antiviral Defense: Implementing Agency-Wide Virus Detection Programs and Procedures to Lower Virus Fakery. Antivirus software, regular file backups, the use of write-protected programme media (diskettes, CD-ROMs), and verifying the source of software before installing it on CDs or other media brought from home or any other outside source are all essential measures for all agencies to take to protect their network from the introduction or spread of computer viruses.

Both our national and economic security are vulnerable to cybercriminal activity. The Federal Bureau of Investigation (FBI) has a plan in place to deal with cyber threats that involves making life difficult for their adversaries. Our goal is to change the actions of criminals and state actors who now believe they can attack American networks, steal money and intellectual property,

and threaten critical infrastructure with little to no personal consequence. We do this by making use of a special set of legal rights, technical means, and interpersonal connections to punish our cyber enemies. The Federal Bureau of Investigation is in charge of investigating hacking incidents. We gather information, share it, talk to victims, and try to track down the people behind hostile cyber operations wherever they may be.

Ways to go to war?

If we believe that we are victims of an online or internet-enabled crime, we must immediately file a report with the Internet Crime Complaint Centre (IC3). The purpose of filing a police report is to help authorities gather information and conduct investigations. Lost money can sometimes be reclaimed with the help of timely reporting. If you want to learn more about crime and how to avoid becoming a victim, check out ic3.gov.

Connect with the FBI's office in your area.

Those of you who discover that our company has been the target of a network intrusion, data breach, or ransomware attack should report it to the FBI by contacting their local field office or going to tips.fbi.gov.

Contending with Cyber Crime's Changing Face

Our enemies seek entry points into our intelligence and data security systems. The FBI is committed to bridging this gap by collaborating with other government agencies, international organisations, and private businesses.

By working together, we are better able to protect networks, identify the source of attacks, correct wrongdoing, and fight off foreign adversaries. The FBI encourages this team-based approach by creating specialised nodes where the public sector, private enterprise, and educational institutions may forge reliable partnerships to counteract cybercrime.

Focus within the government is provided by the National Cyber Investigative Joint Task Force (NCIJTF). The FBI is in charge of this task force, which consists of over thirty Intelligence Community and law enforcement agencies working together in one location. The NCIJTF is led by top executives from its member organisations and organised into "mission centres" that each focus on a certain area of cyber security vulnerability. In these mission control hubs, actions and intelligence are coordinated to counteract the United States' most dangerous enemies.

Only by cooperation can we ensure our safety, security, and confidence in today's technologically interconnected society.

The Methods We Use

The FBI is always evolving to meet the challenges provided by the dynamic nature of the cyber threat, whether that's through the development of novel investigative methods, the use of cutting-edge analytic tools, or the cultivation of new partnerships within the local community.

Specially trained cyber teams at each of the FBI's 56 field offices work with other agencies as part of interagency task forces.

Within hours of being activated, the Cyber Action Team may respond to major incidents anywhere in the country.

To better pursue justice for victims of malicious cyber activity, the FBI works closely with its international partners, including cyber assistant legal attachés stationed in embassies around the world.

The IC3 is a clearinghouse for public reporting of Internet-related crime. The IC3's Recovery Asset Team has helped cybercrime victims freeze hundreds of thousands of dollars using similar allegations.

CyWatch is the FBI's 24/7 operations hub and watch floor, allowing agents to monitor situations and communicate with local field offices from a central location.

Ensure the Safety of Our Infrastructure and Data

Make sure you're running the most recent versions of all your software, and that you've got a reliable, powerful anti-virus

programme installed.

Create a different, strong password for every one of our online accounts and switch them around regularly. If one of our accounts is compromised, all the others will be at risk because we used the same passphrase for all of them.

Do not access any files, documents, or invoices in an email's attachment unless you are expecting them and have previously dealt with the sender. Hold Fast to Our Links

Avoid making any purchases or other financially significant transactions while connected to a public Wi-Fi network, and use caution when connecting to such networks in general.

Never use the free outlets provided by airports, hotels, or shopping centres to charge your device. Criminals have discovered a way to spread malware and spy apps using public USB ports. We can just plug into an outlet instead than taking our own battery pack and USB cable.

Secure our Financial Information and Personal Details

You should always check the sender's address in an email and the website's address before providing any personal information. In order to trick their victims, scammers will often use nearly identical but slightly misspelt versions of legitimate company names, domain names, and email addresses. Alternatively, an email can look like it came from a reputable company, but the sender's address might be malicious.

Do not visit the website linked to in an unsolicited text message or email asking you to confirm, update, or check your account information. We can check the status of our account at any time by logging in online or by calling the toll-free number provided on the company's website.All requests for electronic payments or transfers of funds must be thoroughly scrutinised.

Any message that insists you respond immediately should be treated with suspicion.When making transactions online, credit cards provide an extra safeguard against unauthorised usage.Do not give out our bank account information or send money to anybody we have only met online.

We will submit an IC3 Report if we are a victim.

If we believe that we are victims of an online or internet-enabled crime, we must immediately file a report with the Internet Crime Complaint Centre (IC3). The purpose of filing a police report is to help authorities gather information and conduct investigations. Lost money can sometimes be reclaimed with the help of timely reporting.

If you want to learn more about crime and how to avoid becoming a victim, check out ic3.gov.

Read up on the latest scams and criminal activities that are plaguing the world today. And get the inside scoop on what the Cyber Division is up to.

Please report any suspected scam emails to the Federal Trade Commission. Have you gotten a suspicious message? If you want to help protect others, you should let the FTC know.

CONCLUSION:

This study concludes that as the prevalence of cybercrime rises, more detection mechanisms and user education on online safety must be implemented, coupled with comprehensive instruction on the advantages and downsides of the Internet before accessing it. There is no doubt that the Internet provides several chances for crooks. Information is the most effective kind of defence. In order to secure computer systems from cyber attacks, it is necessary to devise methods for preserving and tracking electronic evidence. In addition, new cyber laws and policies must be devised to combat the many types of cybercrime. Even businesses must take the necessary precautions to examine and protect their interest.

REFERENCES

1. Kshetri, N., Pattern of global cyber war and crime: A conceptual framework. Journal of International Management, 11(4), pp.541-562. (2005)
2. Reuters, Cybercrime costs global economy $445 billion a year: report. Available at:https://www.reuters.com/article/us-cybersecurity-mcafee-csis-idUSKBN0EK0SV20140609 [Accessed on: 9th September 2022] (2014)
3. Sunakshi Maghu, Siddharth Sehra and Avdesh Bhardawaj. Inside of Cyber Crimes and Information Security: Threats and Solutions. pp. 835-840 Available at: https://www.ripublication.com/irph/ijict_spl/ijictv4n8spl_09.pdf [Accessed on: 9th September 2022] 2014
4. Hindubusinessline, Corporate Espionage via social media Rampant In India Inc.: Assocham Survey. Available at: https://www.thehindubusinessline.com/companies/Corporate-espionage-via-social-media-rampant-in-India-Inc-Assocham/article20455145.ece [Accessed on: 9th September 2022] (2017)
5. Prague post, Cyber terrorism and politically motivated computer crime are a big concern for the real world. Available at: https://www.praguepost.com/opinion/5996-virtual-hostage.html [Accessed on: 9th September 2022] 2014
6. Choi, K.S. and Lee, C.S.,. The present and future of cybercrime, cyberterrorism, and cybersecurity. International Journal of Cybersecurity Intelligence & Cybercrime, 1(1), pp.1-4. 2018
7. Nzeakor, O.F., Nwokeoma, B.N. and Ezeh, P.J.,. Pattern of cybercrime awareness in Imo state, Nigeria: An empirical assessment. International Journal of Cyber Criminology, 14(1), pp.283-299. 2020.