International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 7, Issue 2, February 2022, http://ijmec.com/

"CYBER CRIME CHANGING EVERYTHING – ANEMPIRICAL STUDY"

Srikanth Bhyrapuneni [1], T. Srinivasulu [2], Harikrishna Chilakala [3]

[1]Assistant Professor, Department of CSE, RISE Krishna Sai Gandhi Group of Institutions, Ongole, [2]Assistant Professor, Department of CSE, RISE Krishna Sai Prakasam Group of Institutions, Ongole, [3] Associate Professor, Department of CSE, RISE Krishna Sai Gandhi Group of Institutions, Ongole.

Abstract— The Internet is often described as awonderful tool, an engaging place and a become victims to the growing pool of criminals who skilfully navigate the Net. Cyberspace often known as Web is an environment that is intangible and dynamic.This paper argues that Cyber Crime or e – crimepresents a new form of business and Hi-tech Criminals.

This paper explores an overview of Cyber Crimes, the cyber- crime perpetrators and their motivations also I want to discuss in detail of different cyber crimes, and unique challenges and response issue which may be encountered during the prevention, detection and investigation and also outlined the different section of IT Act 2000 of India also proposed new provision in IT Act 2000.

Keywords— Cybercrime, Hackers, Crackers, Child Pornography, Viruses, Worms, Trojans, Cyberstalking, Cyber Defamation, Cyber Law, India, IT Act 2000.

Introduction: The Internet changes everything. It"s upset our notions of how things should be, how countries should begoverned, how companies should be run, how teachers teachand children learn, and even how housewives make new recipes. It mixes up our conceptual framework of what wethink we know about the world, about each other and about ourselves. It is liberating, exciting, challenging and terrifying all at the same time. To a majority of the people, the Internet remains mysterious, forbidding, incomprehensible and frightening. Along with the phenomenal growth of theInternet has come the growth of cyber- crime opportunities.As a result of rapid adoption of the Internet globally, computer crimes include not only hacking and cracking, but now also include extortion, child pornography, money laundering, fraud, software pirating, and corporate espionage, to name a few.Law enforcement officials have been frustrated by the inability of legislators to keep cyber crime legislation ahead of the fast-moving technological curve.

At the same time, legislators face the need to balancethe competing interest between individual rights, such as privacy and free speech, and the need to protect the Further complicating cyber crime enforcement is the area ofLegal Jurisdiction. Like pollution control legislation, one country cannot by itself effectively enact laws that comprehensively address the problem of Internet crime without cooperation from other nations.

Law enforcementagencies around the world are working together to develop new partnership, new forensic methodologies and newresponses to cyber crime in order to ensure safety and security on the Internet. Due to its global dimensions and borderless nature, new and innovative responses are required to the issue of

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 7, Issue 2, February 2022, http://ijmec.com/

cybercrime or e-crime or computer crime.

However, this paper argues that e-crime, and particularly „hi-tech crime", presents a new form of business that will requirea fundamental paradigm shift in policing. In section 2 and 3 of this article, we begin by providing an overview of ybercrimes, and cybercrime perpetrators and theirmotivations. Then in Section 4 we have discuss the different type of cybercrimes and then in Section 5 we identified and discuss the new and uniquechallenges and response issued which may e encountered during the prevention, detection and investigation of suchcrimes and further in Section 6 and 7 we outline what IT Act2000 of India is doing to prevent and reduce the incident of this type of crime and enhance the safety and security of our communities. In Section 8, we proposed the changes in IT Act 2000 and finally, we conclude this paper with a brief statement on the cybercrime and its challenges.

Background

What is the Cyber Crime? Some experts believe that cyber- crime is nothing more than ordinary crime committed by high tech computers where computer is either a tool or target or both and other experts view that cyber-crime is a new category of crime requiring a comprehensive new legal framework to address a unique nature of emerging technologies and the unique set of challenges that traditional crime do not deal with such as jurisdiction, international

The Perpetrators – Hackers & CrackersHackers

Hacker is a term commonly applied to a "Computer use who intends to gain unauthorized access to a computer system." According to IT Act 2000 section 66 a person whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects its inuriously by any means is a hacker.

Crackers

A "cracker" is a hacker with criminal intent. According to the Jargon Dictionary this term is used to distinguish "benign" hackers from hackers who maliciously cause damage to targeted computers. Crackers maliciously sabotage computers, steal information located on secure computers and cause disruption to the networks for personal or political motives.

Why People Hack

Cyber crime presents a "*new forms of business"* will be characterized by new forms of crime, a far broader scope and scale of offending and victimisation, the need to respond in much more timely way, and challenging technical and legal complexities. So hacking involve different personal, political or professional motives

1. **Hactivism**

In recent years it is seen that Hacktivists launch businessmotivated attacks on public web pages or e-mail servers.The hacking groups and individuals, or hacitivists overload email servers by sending massive amounts of e-mails to one address and hack into websites to send a professional orbusiness messages.

2. **Employees**

In a study it is found that disgruntled employees are the greatest threat to a computer security. Employees steal confidential information and trade secrets for the financial benefits. According CBI (Cyber crime cell) disgruntled insiders are a major source of computer crimes. Insiders do not need a great deal of knowledge.

Recreational Hackers

"Recreational hackers" break into computer networks forthe thrill of the challenge or for bragging rights in the hacking community. The recreational hacker download attack script and protocols from the Internet only and launch them against the victim sites with little knowledge of thesystems they are attacking

Types of Cyber Crime

A computer is an indispensable tool for almost all cybe-

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 7, Issue 2, February 2022, http://ijmec.com/

crimes. However, as more devices are enabled to communicate with the Internet, the hackers arsenal of tools is likely to multiply. A computer can be the target of the offense, the tool used in the offense, or may contain evidence of the offense. The different uses of computer will results tothe criminal statutes. When a computer is the target of the offense, the criminal goal is to steal information from, orcause damage to, a computer, computer system, or computer network. Hacking, cracking, espionage, cyberwarfare, and malicious computer viruses arecommon forms of crimes that target the computer. The perpetrators may be teenage, students, professional or the terrorists.

The computer may also be the tool of the offense. The cyber criminals uses the computer to commit a traditional crime such as to print fake currency using advanced color printers. Computers can also be incidental to the offense, but are nevetheless important because they contain the evidence of a crime. For example Child pornographer‟ computers may contain the produced, possessed, received, and/or distributed child pornography. Money Launderers, may use a computer to store details of their laundering operation instead of relyingon paper accounting records.

Malicious Code – Viruses, Worms and Trojans

Viruses

A virus is a program that modifies other computer programs. These modifications ensure that the infected program replicates the virus. Not all viruses cause damage to its host. Avirus is typically spread form one computer to another by e- mail, or infected disk. However a virus cannot infect another computer until the program is executed. A common method of virus execution is when a computer user is tricked intoopening a file attacked to an e-mail, thinking the file is a harmless program coming from a friendly source. The most popular example of virus is the Melissa virus which was launched in March 1999. The Melissa virus was hidden in a Microsoft word attachment that appeared to come from a person knows to the recipient. The program activated a macro that tread the first fifty e-mail addresses located in the Microsoft Outlook e-mail program and e-mailed itself to the fifty addresses. The virus was estimated to have caused $80 million in damages.

Worms

A worm is stand alone program that replicates itself. A worm can wind its way throughout a network system without the need to be atttached to a file, unlike viruses. For example I loveYou worm in 2001 was estimated the loss caused to be $US 10.7 billion.

Trojan Horses

A Trojan Horses is a an innocent looking computer program that contains hidden . That will perform an unauthorized function. A Trojan horse is the most common way in which viruses are introduced int computer systems. For example Back Orifice 2000 is a program designed for misuse and attack on another compute

Denial of Service

A Denial of Service (“DoS”) is an attack or intrusion designed for use against computers connected to the Internetwhereby one user can deny service to other legitimate users simply by flooding the site with so much traffic that no other traffic that no other traffic that no other traffc can get in or out. The hacker isn‟t necessarily trying to break in to the system or steal data data but rather prevent users from accessing their own network for reasons only the hacker knows; revenge, ecnomical orpolitical gain, or just plain nastiness. For example Yahoo, Amazon.com, Buy.com and others.

Cyberstalking

Cyber stalking is when a person is followed and pursued

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 7, Issue 2, February 2022, http://ijmec.com/

online. Their privacy is invaded, their every move watched. Itis a form of harassment, and can disrupt the life of the victim and leave them feeling very afraid and threatened. Stalking or being 'followed' are problems that many people, especiallywomen, are familiar with. Sometimes these problems (harassment & stalking) can occur over the Internet. This is known as cyber stalking. The internet mirrors the real world. That means it also reflects real life & real people with real problems. Although it is rare, Cyber stalking does occur. Cyber Stalking usually occurs with women, who are stalked by men, or children who are stalked by adult predators orpaedophiles. A cyber stalker does not have to leave his home to find, or harass his targets, and has no fear of physical violence since he believes he cannot be physically touched in cyberspace. He maybe may be on the other side of the earth or a neighbour or even a relative! And a stalker could beof either sex. Typically, the cyber stalker's victim is new on the web, and inexperienced with the rules of netiquette & internet safety. Their main targets are the mostly females, children, emotionally weak or unstable, etc. It is believed that Over 75% of the victims are female, but sometimes men arealso stalked. The figures are more on assumed basis and the actual figures can really never be known since most crimes of such natures go unreported.

Financial crimes

This would include cheating, credit card frauds, money laundering etc. To cite a recent case, a website offered to sellAlphonso mangoes at a throwaway price. Distrusting such a transaction, very few people responded to or suppliedthe website with their credit card numbers. These people were actually sent the Alphonso mangoes. The word about this website now spread like wildfire. Thousands of people from all over the country responded and ordered mangoes by providing their credit card numbers. The owners of what was later proven to be a bogus website then fled taking the numerous credit card numbers and proceeded to spend hugeamounts of money much to the chagrin of the card owners.

Cyber pornography

This would include pornographic websites; pornographic magazines produced using computers (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc). Recent Indian incidents revolving around cyber pornography include the Air Force Balbharati School case. A student of the Air Force Balbharati School, Delhi, was teased by all his classmates for having a pockmarked face. Tired of the cruel jokes, hedecided to get back at his tormentors. He scanned photographs of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. It was only after the father of one of the class girls featured on the website objected and lodged a complaint with the police that any action was taken. In another incident, in Mumbai a Swiss couple would gather slum children and then would force them to appear for obscene photographs. They would then upload these photographs to websites specially designed for paedophiles. The Mumbai police arrested the couple for pornography

Sale of illegal articles

This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or 167 simply by using email communication. E.g. many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'.

Online gambling

There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

Intellectual Property crimes

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 7, Issue 2, February 2022, http://ijmec.com/

These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc.

Email spoofing

A spoofed email is one that appears to originate from onesource but actually has been sent from another source. E.g. Pooja has an e-mail address pooja@asianlaws.org. Herenemy, Sameer spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Pooja, her friends could take offence and relationships could be spoiled for life. Email spoofing can also cause monetary damage. In an American case, a teenager made millions of dollars by spreading false information aboutcertain companies whose shares he had short sold. This misinformation was by sending poofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies weredoing very badly. Even after the truth came out the values ofthe shares did not go back to the earlier levels and thousands of investors lost a lot of money.

Forgery

Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. Outside many colleges across India, one finds touts soliciting the sale of fake mark sheets or even certificates. These are made using computers, and high quality scanners and printers. In fact, this has becoming a
booming business involving thousands of Rupees being given to student gangs in exchange for these bogus but authentic looking certificates.

Cyber Laws in India

In May 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President in August 2000 and came to be known as the Information Technology Act, 2000. Cyber laws are contained in the IT Act, 2000. This Act aims to provide the legal infrastructure for e-commerce in India. And the cyber laws have a major impact for e-businesses and the new economy in India. So, it is important to understand what are the various perspectives of the IT Act, 2000 and
what it offers. The Information Technology Act, 2000 also aims to provide for the legal framework so that legal sanctity is accorded to all electronic records and other activities carriedout by electronic means.

Advantages of Cyber Laws

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records

In view of the growth in transactions and communicationscarried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic

records / communications through digital signature.

Proposed Changes in IT Act 2000

It is found that there should be the provision for the following

a. Trap and Trace orders. The new IT Act should make such legislation that it ishacking assault is to follow a chain of trapping devices that logged the original malicious packets as they arrived at eachindividual router or server. In a case of single telephone company, it has been relatively easy for investigators to obtain trap and trace orders but today one communication is being carried byseveral different {ISPs}, by one or more telephone company or one or more cell company and very soon by one or more satellite company. Once the

then go the next jurisdiction and file a request for a trap and trace order for the next segment. The new legislation would authorize the issuance of a single order to completely trace an on-line communication from start to finish.

b. We proposed new legislation such that makes young perpetrators fifteen years of age and older eligible for offencesin serious computer crime.

c. The Cyber Cafes, Computer Training Centre, and other Institute where computer is the mode of training should be incorporated under some act.

CONCLUSIONS

In essence, our empirical study underscores the urgency of addressing cybercrime comprehensively and collaboratively. Cybercrime is not a static problem; it is an ever-evolving ecosystem that demands constant vigilance, adaptation, and innovation. It is imperative that governments, businesses, and individuals work together to fortify our digital defenses, protect our privacy, and preserve the integrity of the digital world we increasingly rely upon.

Acknowledgment

Criminal behavior on the Internet, or cyber crime, presents as one of the Major challenges of the future to India and International law enforcement. As ICT become even more pervasive, aspects of electronic crime will feature in all forms of criminal behavior, even those matters currently regarded as more traditional offences. It already feature in many international crime involving drug trafficking, people smuggling, terrorism and money laundering. Digital evidence will become more commonplace, even in traditional crimes, and we must be prepared to deal with this new challenge. Law enforcement agencies around the world are working together to develop new partnerships, new forensic methodologies and new responses to cyber crime in order to ensure safety and security on the Internet. New skills, technologies and investigative techniques, applied in a global context, will be required to detect, prevent and respond to cybercrime. This „new business" will be characterized by new forms of crime, a far broader scope and scale of offending and victimisation, the need to respond in much more timely way, and challenging technical and legal complexities.

REFERENCES

1.ETTER,B. (2001), THE FORENSIC CHALLENGES OF E- CRIME, CURRENT COMMENTARY NO. 3 AUSTRALASIAN CENTRE FOR POLICING RESEARCH, ADELAIDE.

2.Etter B. (2002), The challenges of Policing Cyberspace, presented to the Netsafe:Society, Safety and the Internet Conference, Auckland, NewZealand.

3.Eric J. Sinrod and William P Reilly, Cyber Crimes (2000), A Practical Approachto the Application of Federal Computer Crime Laws, Santa Clara University, Vol16, Number 2.

4.Gengler, B. (2001), Virus Cost hit $20bn, The Australian, 11 September p.36.

5.The IT Act 2000.

6.Cyber stalking India, www.indianchild.com.

7.Cyber crime a newchallenge for CBI, www.rediff.com, March 12, 2003 12:27 IST

8.Richard Raysman & Peter Brown (1999), Viruses Worms, and other Destructive Forces N. Y. L. J.

9.Kabay, M. E. (2000). Studies and Surveys ofComputer Crime, Focus. http://securityportal.com/cover/coverstory2001211.html

10.KPMG (2000) , E-Commerce and Cyber Crime: New Strategies for Managing theRisks of Exploitation, USA

11.Legard, D (2001), Hackers Hit Government Sites, Computer World, Vol 24 No. 26, 29 Jan, p.12.

12.Russell G. Smith, Peter Grabosky and Grgor Urbas, 0521840473 – Cyber Criminals on Trial, Cambridge University Press.

13.Seamus O Clardhuanin (2004), An Extended Modelof Cybercrime Investigations,International Journal of Digital Evidence, Summer 2004, Vol3, Issue 1.