Addressing The Growing Threat of Cyber Crime in India: Challenges and Solutions

• MITR RAO
G.D. GOENKA UNIVERSITY, HARYANA, INDIA

FOR EVERY LOCK, THERE IS SOMEONE OUT THERE WHO IS TRYING TO PICK IT OR BREAK IN.

-DAVID BERNSTEIN

Cybercrime is crime committed on the Internet, using the Internet and by means of the Internet. With the growth of the Technology and the evolution of the Internet, along came another revolution of crime where the perpetrators commit acts of crime and wrongdoing on the World Wide Web. Computer crime or cybercrime refers to any crime that involves a computer and a network (Moore 2005). Individuals or groups can exploit the anonymity afforded by cyberspace to engage in illegal or illicit activities that aim to intimidate, harm, threaten or cause fear to citizens, communities, organizations or countries. Internet crime takes many faces and is committed in diverse fashions. Cyber stalking, spreading computer virus, Cyber trafficking, Child sex offences (pornography and grooming), Crimes in virtual world Cyber activism, Virus writing and malware, Identity theft, Internet Fraud, Illegal financial transactions, Money laundering, Serious acts of Cyber bullying etc. Although most members of society are aware of the Internet as a platform and understand its huge potential. The challenge for the society of the 21st century is to take advantage of these opportunities, while at the same time protect itself from the risks inherent in use of web. Authors believe that, there is a need to push for stricter control and regulation on cyber activity. A higher Internet literacy level can help people protect themselves even better by taking simple security measures, such as using anti-virus software and identifying potential risks or scams in their online financial transactions. Now is the time to launch an initiative to develop a strategic roadmap to address malicious cyber activity in a proactive way by the government and the organization at National and International Level. In this paper Authors have suggested various preventive measures to be taken to snub the cybercrime in India which includes proper regulation of security of Internet, Cyber cell to tackle problem of Hacking, Strong system of Banking awareness amongst the internet users' regulation of cyber. And any cybercrime is committed than complete justice must be provided to the victims of cybercrimes by way of compensatory remedy and offenders to be punished with highest type of punishment so that it will anticipate the criminals of cybercrime. Yet India has taken a lot of steps to stop cybercrime but the cyber law cannot afford to be static, it has to change with the changing times.

Keywords | Cyber Crime, Internet, Control Measures, Cyber fraud, Prevention of cybercrime.

Introduction

"Cybercrime is a criminal offence on the Web, a criminal offence regarding the Internet, a violation of law on the Internet, an illegality committed with regard to the Internet, breach of law on the Internet, computer crime, contravention through the Web, corruption regarding Internet, disrupting operations through malevolent programs on the Internet, electric crime, sale of contraband on the Internet, stalking victims on the Internet and theft of identity on the Internet.[1] The computer age gave rise to a new field of crime namely "cybercrime" or "computer crime". During the 1960s and 1970s cybercrime involved physical damage to the consumer system. Gradually computers were attacked using more sophisticated modus operandi where individuals would hack into the operating system to gain access to consumer files. The 1970s - through to the present - saw cybercrimes taking different trajectories like impersonation, credit card frauds, identity theft, and virus attacks, etc.[2]

The use of the internet in India is growing rapidly. According to a recent Telecom Regulatory Authority of India (TRAI) survey, we currently have 20.33 million internet subscribers.[3] While burgeoning growth in the use of internet provides multiple options to cyber citizens in all possible spheres– from entertainment to education, it has also given rise to cybercrime. This new breed of tech-savvy fraudsters pose a new set of challenges. Over the past ten years, crime (traditionally based in the world of physical entity) has been increasingly making its way into the world of information. Crime is evolving; since the days when goods were transported by stagecoach, robbery has changed to keep up, even to our modern-day equivalent credit and debit cards. Internet credit card number theft has become a well-recognized danger. The most common forms of computer crime reported to Inter-GOV include child pornography, fraud, and e-mail abuse. Even more disturbing are new forms of cyber-terrorism made possible by the large amount of the physical machinery now operated by computers. In this article, after attempting to define computer crime, we examine the types that have been committed in the past, and the new types likely to appear in the future. We also

[1] http://legal-dictionary.thefreedictionary.com/cybercrime
[2] http://www.mekabay.com/overviews/history.pdf
[3] http://www.trai.gov.in

examined the difficulty in detecting and measuring computer crime, methods for attempting to prosecute or prevent such crimes, and the effectiveness of these measures. [4] Internet is believed to be full of anarchy and a system of law and regulation therein seems contradictory. However, Cyberspace is being governed by a system of law called Cyber law. Cyber law is a generic term which refers to all the legal and regulatory aspects of Internet. Cybercrime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cybercrime has assumed rather sinister implications This article evaluates the concepts of computer crimes, detection and the controls. The paper evaluates the dangers of cybercrime which it poses to organizations, factors that encourage it, and recommending possible controls and preventive measures against computer crimes.

Dynamic Crime in 21st Century

Cybercrime rates continue to increase in line with Internet adoption: mobile Internet access and the continuing deployment of broadband Internet infrastructure throughout the world therefore introduces new levels of vulnerability; with potential victims online for longer periods of time and capable of transmitting much more data than before; and the increasing trend for outsourcing data management to third parties presents imminent risks to information security and data protection. In the last decade advances in communications technologies and the "information" of society have converged as never before in human history. This has given rise to the industrialization of a type of crime where the commodity, personal information, moves far too quickly for conventional law enforcement methods to keep pace. The unprecedented scale of the problem threatens the ability of the authorities to respond with millions of viruses and other types of malicious code are in global circulation, and again innumerable computers are compromised per day.[5] Today computers have come a long way, with neural networks and nano-computing promising to turn every atom in a glass of water into a computer capable of performing a Billion operations per second. Cybercrime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cybercrime has assumed rather sinister implications.[6] Major Cybercrimes in the recent past include the Citibank rip off. US $ 10 million were fraudulently transferred out of the bank and into a bank account in Switzerland. A Russian hacker group led by Vladimir Kevin, a renowned hacker, perpetrated the attack. The group compromised the bank's security systems. [7]

Challenges and Impacts of Cyber Crime

The threat from cyberattacks and malware is not only apparent, but also worrisome. Attackers are compromising computer systems in different parts of the world and use masquerading techniques and hidden servers to hide the identity of actual systems from which the attacks are launched. Target audience of hackers are evolving , for example, high-net-worth individuals can be now be easily identified through a vista of social media channels that allow attackers to ascertain certain online patterns and the cyber behaviour of these individuals.[8] Cyber-crimes or crimes committed in the virtual world of the Internet wherein "the computer is either a tool or target" is the most pervasive of all forms of privacy intrusions in the modern world. Owing to the extensive use of the Internet and technological up gradation in the e-world people use the Internet for a wide variety of purposes which include social networking sites such as Facebook, Twitter, LinkedIn. These sites have more than 400 million users and applications such as chatting, uploading, photographs and others have the capacity to retain a lot of private information in their databases[9].

Legal Framework and Issues in India

Also, the "Cyber Law of India" has been subject to amendments on various occasions but hasn't served the changing dynamics and the growing threats and manifestations of cyberwar. The need of the hour for India is to formulate preventive strategies to curb cybercrimes effectively as well as impart cybercrime investigation training and technological know-how to the various law enforcement agencies.[10] Some of the key areas which need to be dealt with are cyberwarfare, cyberterrorism, cyberespionage and international cybersecurity cooperation that would enable developing nations to gather technical expertise from the developed ones to tackle the ever-growing threat to cybersecurity. Various reports from security and analyst firms suggest that India will continue to become a strategic target, as attackers are exploiting gaps to compromise critical networks, and that Indian organisations are more likely to be exposed to attacks than the global average. Digitization will only expose more sensitive data to threat groups who want to seek access to intellectual property, intelligence and critical infrastructure for financial gains. Cyber criminals from around the world are involved in hacking and launching attacks on computer networks of Indian organisations. The government will need to focus on creation of laws related to the use of ICT, protection of intellectual property and access to digital content, among other

[4] http://www.isea.gov.in/isea/index.jsp
[5] http://ijcsit.com/docs/Volume%204/Vol4Issue5/ijcsit2013040519.pdf
[6] https://www.ncsc.gov.uk/
[7] https://www.bsi.bund.de/EN/Home/home_node.html
[8] http://epaperbeta.timesofindia.com/article.aspx?eid=31816&articlexml=securing-digital-india-19022016007005
[9] http://shodhganga.inflibnet.ac.in/bitstream/10603/49514/12/12_chapter%205.pdf
[10] Rebovich, Donald et. al. The National Public Survey on White Collar Crime. Morgantown, WV; National White Collar Crime Center, 2000.

parameters for the success of 'Digital India'.[11] A holistic data protection regime needs to be incorporated in the law to make it more effective. Taking lead from the Five Year Plan, the Department of Electronics and Information Technology (DeitY), India has also defined a cybersecurity strategy.[12] DeitY states that the risks associated with current and anticipated vulnerabilities of, threats to, and attacks against the IT infrastructure provide the rationale for this strategy. The primary objectives of DeitY's cybersecurity strategy revolve around three primary objectives, which are supported by five actions and strategic initiatives. The current cybersecurity strategy of DeitY mostly focuses on the areas as defined in the Five Year Plan.[13] However, positive steps have been taken by the government, especially in wake of recent surge in adopting digital technology for governance and providing citizen-centric services. It is worth mentioning that currently only a few nations have successfully put into motion, strategic initiatives for cybersecurity. The IT Act 2000 was enacted by the government in 2000 to punish acts of cybercrime. The Act was amended in the year 2008. According to the National Crime Records Bureau, cybercrime is on the rise. The Bureau reported that 420 cases were reported under the IT Act in the year 2009 alone, which was a 45.8 per cent increase from the year 2008.[14] The NCRB data on cybercrime also provides a useful insight as to the growing awareness of the IT Act. The data clearly shows an increase in the number of cases reported from the years 2005 to 2009. Hacking and obscene publication/transmission are the highest reported crimes with the highest rate of conviction under the IT Act 2008.[15] Cybercriminals can gain access to financial data, compromise intellectual property of companies, tap sensitive national data and steal government records. These actions could compromise national security and interests. India has struggled to cope with the implementation of its cybercrime laws. The country has approved amendments11 to its IT Act, 2000; however, technology has grown leaps and bounds complicating legal response and calls for a review. The IT Act penalizes various cybercrimes and provides punishments (imprisonment terms up to 10 years and fines up to INR1 crore, in some cases). The IT (Amendment) Act, 2008[16] , has included the following: Electronic signatures ,Corporate responsibility, Definitions of important terms, such as intermediaries and communication devices , Legal validity of electronic documents, Role of adjudicating officers, Requirements on data retention[17] The amendment introduced in 2008 Act does not really bring about much change with respect to encryption, except for expanding the scope of the government's power to order decryption. While earlier, under section 69, the Controller had powers to order decryption for certain purposes and order 'subscribers' to aid in doing so (with a sentence of up to seven years upon non-compliance). Now, the government may even call upon intermediaries to help it with decryption (section 69 (3)). [18]Additionally, section118 of the Indian Penal Code has been amended to recognize the use of encryption as a possible means of concealment of a 'design to commit [an] offense punishable with death or imprisonment for life'[19]. While such legal mechanisms are being developed, companies in India will need to increase investments to safeguard themselves against cybercrime. One of the key impacts is the increasing cost to recover from cyber fraudulence or data breaches. Other negative fallouts of cybercrime to a business include damage to brand and other reputational losses, and harm to customer relations and retention.[20]

Measures at International Level

Some mature countries have leveraged partnership with private players and industry to equip them to counter the menace of cybercrime. For example, countries already have existing bodies or agencies, which are privately-led, but are supported by government agencies. For example, in the USA, a privately-led Identity Ecosystem Steering Group (has been established to support the National Strategy for Trusted Identities in Cyberspace. Similarly, the Australian Government has established the Trusted Information Sharing Network for Critical Infrastructure Resilience.[21] It is Australia's primary national engagement mechanism for business-government information sharing and resilience building initiatives on critical infrastructure resilience.[22] For the past two decades, the international community has focused on the development of extradition treaties, mutual legal assistance treaties, and sanctions to combat the proliferation of money laundering crimes on an international scale. The international focus for the next two decades must be directed toward Internet crime and cybercrime. That focus cannot be limited to procedural remedies. Many countries lack substantive laws specifically designed to combat computer and Internet crimes. For example, the alleged perpetrators of the "Love Bug" virus in the Philippines could not be charged with a substantive crime because no computer crime laws had been enacted in that country. The international community must maintain a more aggressive and comprehensive approach to cybercrime, including treaties that provide for uniform laws on cybercrime and cyber terrorism. That approach should

[11]http://epaperbeta.timesofindia.com/article.aspx?eid=31816&articlexml=securing-digital-india-19022016007005

[12] Gupta, Rohit K. (2013). India : An Overview of Cyber Laws vs. Cyber Crimes : In Indian Perspective at www.mondaq.com accessed on 7th March ,2017

[13]http://assocham.org/upload/event/recent/event_1168/Strategic_national_measures_to_combat_cybercrime_Report_light_version.pdf

[14] http://www.cyberlaws.net/itamendments/index1.htm

[15]http://ncrb.nic.in/CII%202009/cii2009/Chapter%2018.pdf

[16]http://meity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf

[17]https://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Pages/default.aspx

[18]http://www.itu.int/ITUD/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

[19] Weigel, Margaret (2013). The State of Internet Privacy in 2013: Research round up at www.journalistsresource.org/another/margaret-weiget. Accessed on 25th Feb,2017

[20] http://meity.gov.in/content/technology-trendsz

[21] Sutherland, Edwin H. White Collar Crime. NY: Dryden Press, 1949.

[22] American Association of Retried Persons, Findings from a Baseline Omnibus Survey on Telemarketing Solicitation. Washington, DC: AARP, 1996.

be inspired and led by the United States. On April 27, 2000, the Council of Europe released a draft version of its proposed International Convention on Cyber-Crime. In 1989 and 1995, the Council encouraged member governments to revise or adopt laws specific to the challenges of computer crime.[23] However, a binding legal agreement is now considered necessary to harmonize computer crime laws and to step up investigations and ensure effective international cooperation. The Council hopes to adopt the Convention by September 2001.[24] The Convention draft requires each signatory nation to adopt legislation or other measures with respect to five categories of crimes: ·Offenses against computer data and systems;[25] · Computer-related forgery; · Computer-related fraud; · Child pornography; and · Copyright and intellectual property offenses.

Challenging Privacy and Individuality

A major problem of cybercrime against individual can take place towards different types of people such as cybercrime against children, cybercrime against consumers and cybercrime against normal users. It is clear that cybercrime against children is the most significant issue which should be focused on. [26]One of the main areas of cybercrime is child pornography, which is the documented sexual abuse of children, however this excludes pseudo-photographs or computer generated items such as images, drawing, cartoons and painting (Akdentiz, 2008:4). Â Newville (2001) points out that the internet has authorized to child pornography by offering offenders many ways of swapping information without restraint and giving them a chance of learning and improving skills illegally. [27] Thus, under a high activity by predators of finding open contacts with young victims such as teenagers, a rise in the number of children who use the internet and spread child pornography that cause a serious threat to the safety of children.[28] There are several ways that predators used to meet their young victims in public place and one of the common ways is chartrooms (Medaris and Girouard, 2002). Privacy does not exist in cyber space. The various websites that offer varied services to its consumers fail to protect their personal data time and again. The Sony website including its play station and music website was hacked at least three times this year. Scores of personal data was stolen and the consumers were kept in dark regarding the breach for almost a week. Speaking as a consumer, if a large corporate company like Sony cannot protect its website from being hacked into, it is hard to imagine other websites protecting itself from attacks.

The rise of the Internet has brought with it a new dimension of crime. The IT Act 2000 has brought some reprieve to the aggrieved according to the NCRB. Despite this, the IT Act clearly will not completely deter criminals from hacking into websites, as was demonstrated in the NCRB report. The cyber criminals of the February 2000 cyber-attacks have yet to be apprehended and the attacks on various websites have been increasing every year. [29] Despite progress being made on enacting cyber laws and implementing them, cyber-crime is still not nipped in the bud. Governments can do precious little to stop it and only hope that a cyber-criminal can be traced back and be punished.[30] Hence, Internet users need to more careful of the sites they visit; know the privacy policy of these websites to protect their personal data as much as possible.

Challenges and Solutions

Challenges

- Active targeting of underground fora to disrupt the circulation of powerful and easy to use cyber-criminal tools, such as malware kits and botnets.
- Disrupt the infrastructure of malicious code writers, specialist web hosts through the active identification of developer groups and a joint action of law enforcement, governments and the Information & Communication Technology industry to dismantle so-called "bullet proof" hosting companies.
- Ransom-ware is another concern that has emerged as one of the most troublesome malware categories. The threat is known for locking computers or encrypting files to compel users into handing over their money.
- There are gaps in the availability of proficient cyber experts within law enforcement agencies and the lack of appropriate implementation of the strategy means that a very few measures are in place to immobilize a larger set of cyber sleuths to counter the menace of cybercrime.

Solutions

The strategy and execution of cybersecurity needs to be developed with clear vision for addressing challenges related with cybercrime in the short-term and mid-term with possible review mechanism to a long-term approach in this domain. The global practices from mature law enforcement organizations, such as the Federal Bureau of Investigation (FBI) and Interpol need to be leveraged and adopted as per their feasibility as part of the Indian cybercrime strategy.

[23] Pfister. "Be on the Lookout for ID Thieves," Denver Business Journal, October 1, 1999, 51:6, p. 13A.
[24] Hazlewood, Sara. "Tech Firms Watching Trade Secret Trials," Business Journal Serving San Jose & Silicon Valley, May 14, 1999, 17:2, p. 7.
[25] Hazlewood, Sara. "Tech Firms Watching Trade Secret Trials," Business Journal Serving San Jose & Silicon Valley, May 14, 1999, 17:2, p. 7.
[26] Genderen, Rob van den Hoven van (2008),Cybercrime Investigation and the Protection of Personal data and Privacy, Report for Economic Crime Division, Directorate General of Human Rights and Legal Affairs, Strasbourg,France at www.coe.int/cybercrime accessed on 25th Feb,2017
[27] https://www.ukessays.com/essays/information-technology/cybercrime-problems-and-solutions-information-technology-essay.php
[28] Westin, Alan F. (1967). Privacy and Freedom, Athenum, New York.
[29] http://cis-india.org/internet-governance/cyber-crime-privacy#8
[30] Valentine, Pamela (2001). Cyber Stalking Privacy Intrusion at its Scariest, SANS Institutes Infosec Reading Room at www.sans.org/reading-room-cyber-stalking-privacy-intrusion-itsscariestaccessed on 18th March ,2017

- Active targeting of the proceeds of cyber crime in collaboration with the financial sector. For e.g. money mule (is a person who transfers money acquired illegally (e.g., stolen) in person, through a courier service, or electronically, on behalf of others).
- Continue to develop insight into the behavior of the contemporary cyber-criminal by means of intelligence analysis, criminological research and profiling techniques, and based on the combined law enforcement, IT security industry and academic sources, in order to deploy existing resources more effectively.
- Collaboration, particularly with the private sector, to proactively identify features of future communications technologies liable to criminal exploitation, and to design vulnerabilities out of technologies and environments which are in development.
- More centralized coordination at regional and interregional levels, to streamline the fight against cyber-crime.[31]
- Global Cyber Law should be implemented.
- The establishment of virtual taskforces to target Internet facilitated organized crime.
- In addition to the existing mechanisms, a strategy needs to be documented, which states the vision, objective and approach for cybercrime prevention in India. A definite cybercrime prevention program may originate as a specific recommendation of such a document.
- Parents should be responsible for their children's actions on the internet, however, parents are not able to take this responsibility alone because it is difficult and challenging for them to always stay with their children whilst they are surfing the Internet. Thus, this challenge can be tackled by the close cooperation between parents and governments.
- It is always the parents who have to keep a watch on the sites that your children are accessing, to prevent any kind of harassment or depravation in children.
- Web site owners should watch traffic and check any irregularity on the site. It is the responsibility of the web site owners to adopt some policy for preventing cyber-crimes as number of internet users are growing day by day.
- Strict statutory laws need to be passed by the Legislatures keeping in mind the interest of netizens (cybercitizen or an entity or person actively involved in online communities and a user of the Internet).
- Web servers running public sites must be physically separately protected from internal corporate network.

Conclusion

This Paper has gone some way in explaining the concept of cybercrime as well as addressing two important problems of cybercrime, which are cybercrime against individual such as child pornography and cybercrime against organization such as piracy. Moreover, there are some suggested solutions to each problem that can be met depending on the difficulty of applying and monitoring them. On the other hand, cybercrime is a growing concern throughout the world, thus, research must continue to take place in order to keep cyberspace as safe as possible and protected from the actions committed by cybercriminals. On the other hand, it has been proven that it is the responsibility of the individual to protect his/her own Internet connection. It could therefore be suggested that Governments and local authorities including Police and Education Services should work more closely with the Internet Service Providers to protect minors on the Internet. Despite all the developments in the domain of Child Protection Software, young people will always find a way of avoiding a protective firewall. Therefore, education would serve an important role in protecting children. Furthermore, if the culprits are identified law enforcers could punish and remove the criminals' access to the internet. The misuse of computers is a serious issue in the eyes of the law, and under English Law, the Computer Misuse Act (1990) would be central to prosecuting any individual who attempts to use a computer unlawfully. As Cyber-crime is a new form of crime that has emerged due to computerization of various activities in an organization in a networked environment. With the rapid growth of information technology cyber-crimes are a growing threat. Technology has a negative aspect as it facilitates commercial activity. Ordinarily the law keeps pace with the changes in technology but the pace of technological developments in the recent past, especially in the field of information and technology is impossible to keep pace with legal system. An important concern relates to modernizing penal laws of many countries which predate the advent of computers. On the one hand, the existing laws have to be change to cope with the computer related fraud such as hacking, malicious falsification or erasure of data, software theft, software attacks etc. and on the other, new legislation is also necessary to ensure data protection and piracy. The need for a law on data protection is paramount if India is to sustain investor confidence, especially among foreign entities that send large amounts of data to India for back-office operations. Data protection is essential for outsourcing arrangements that entrust an Indian company with a foreign company's confidential data or trade secrets, and/or customers' confidential and personal data.

[31]http://ijcsit.com/docs/Volume%204/Vol4Issue5/ijcsit2013040519.pd