A REVIEW OF CYBER CRIME: AN EVER GROWING THREAT AND ITS INFLUENCE ON SOCIETY & IT SECTOR

Ashwini Manish Brahme[*]

Sunil B. Joshi*

Abstract

Cyber Crime and Cyber threat is becoming a part of Cyber cold War in toady's IT world and it can cause panic among society, bring down the national sovereignty, break down IT Systems controlling, and organizations too because of this the third world war may found in Cyber space. The paper is mainly intended to discuss Cyber Crime & Cyber Threat, Sectors of cyber crime, Tools used for Cyber threat, and examples. The research paper discuses on an Impact of cyber threat on Society, Nation, Government, and IT sector. This paper briefs on security of society, organization and national sovereignty with a comprehensive framework which suggest AFIT Model for IT Sector and 4'C Model for Security of Society to make awareness of cyber crime, and cyber security and problems to defeat the cyber crime. In addition paper concise on why there is need to report the cyber crime, and where the victim should report and file the cyber crime cases. The research paper also summarizes on role of government to defeat and conquer cyber crime and cyber threat from society and Business.

Keywords

Cyber Crime, PC – Personal Computer, DOS – Denial of Access , ISP - Internet Service Provider , IC^3 - Internet Crime Complaint Center

[*] Assistant Professor, Sinhgad Institute of Management and Computer Application , Pune

I. Introduction : Cyber Crime and Cyber Threat

Computer Technology and use of Internet growing day by day because of low cost of PC and broadband people are using Internet for their business, day to day activities, personal use and may more frequently. There Internet plays vital role all over the globe. People are spending more time on Internet and most of them are not aware of Cyber threats & Cyber Security and directly and directly and indirectly becomes victim of cyber crime and cyber threat. Cyber Crime is an unlawful act where in the computer is either a tool or target used for creation of cyber threat and Cyber threat is threat in Cyber Space which is disruptive activity with the intention of creating threat in social, religion, nation, political and with some specific objective. In more Technical way

Cyber crime is an umbrella term used to refer criminal activity including offences against computer data and systems, computer related offences, content offences and copyright offences. The main objective behind any cyber attack is creating threat in public, destructing government's rules and regulation, attitude of breaking nation's integrity, also to create conflict between religion and languages etc. The Cyber criminal may be children aged between 6-18 years, may be organized hackers, may be professional hacker or cracker, disconnected employees, cheater etc. Cyber criminals may be a person influenced by relationship, stress, and exhausted by unhappiness work, disruption in home life including illness, divorce, and separation. Cybercriminals may be destructive mind person, inspired by the desire to utilize the access, knowledge, privileged or organizational economic or political gain.

- sectors of cyber crime
  - Government and regulators
  - Police
  - Private users
  - Equipment Manufacturers
  - Auditors, Accouters, Fraud Investigators
  - Trusted Third parties, Certification Authorities
  - Corporate Network Operators
- Tools used for Cyber threat
  - Hacking
  - Cryptography
  - Trojans attacks
  - Computer Worms
  - Computer Viruses
  - Denial of service attacks'
  - Email related crimes etc
  - Password Cracker Software's etc.

II. Literature Review

Cyber-crime or computer crime is considered to be any crime that uses a computer and a computer network (Matthews, 2010). A basic definition describes cybercrime as a crime where computers have the possibility of playing an important part (Thomas and Loader, 2000). The main factor in cyber-crime increase is the Internet. By use of Internet, cybercriminals often appeal to images, codes or electronic communication in order to run malicious activities. Among the most important types of Internet crimes we can mention: identity theft, financial theft, espionage, pornography, or copyright infringement.

The cyber-crimes can be divided into two categories: the crimes where a computer network attacks other computers networks – e.g. a code or a virus used to disable a system, and, the second category, crimes where a computer network attacks a target population – e.g. identity theft, fraud, intrusions (Svensson, 2011).

Issues revolving around cyber-crime have become more and more complex. Computer criminal activities have grown in importance and institutions are more interested than ever in putting an end to these attacks. Progressions have been made in the development of new malware software, which can easily detect criminal behavior (Balkin et al., 2007). Moreover, high quality anti-virus systems are offered for free now in many countries at every purchase of a computer or an operating system. Matthews, B. (2010). Computer Crimes: Cybercrime Information, Facts and Resources. This information is taken refereed from http://www.thefreeresource.com/computer-crimes-cybercrimeinformation- facts-and-resources.

A Report by eTechnology Group@IMRB for Internet and Mobile Association In India May 2008 describes about the growth of internet users in India in the various sectors like Home Internet usage in India grew 19% from April 2006 to April 2007. In April 2007 it became 30.32 million and the eMarketer accept that there will be 71 million total Internet users in India by 2011. Rival tradeindia.com has 700,000 registered buyers and it has the growth rate of 35% every year which is likely to double in the year 2008. Indiamart.com claims revenues of Rs. 38 crores and has a growing rate of 50 every year. It receives around 500,000 enquiries per month. Undoubtedly, with the middle class of 288 million people, online shopping shows unlimited potential in India. The real estate costs are touching the sky. The travel portals' share in the online business contributed to 50% of Rs 4800 crore online market in 2007-08. The travel portal MakeMyTrip.com has attained Rs 1000 crores of turnovers which are around 20% of total e-commerce market in India. Further an annual growth of 65% has been anticipated annually in the travel portals alone. As the Internet users are increased it automatically consist of cyber security and its awareness.

Example : Australian website hacked by Atual Dvewedi

The news of cyber crime contains the crime of website hacking published in *www.esakl.com Dated 14 July 2009, Tuesday, Pune ,* Royal Australian Air Force website www.raaf.gov.au hacked by Atual Dvewedi and displayed a message on home page of www.raaf.gov.au Air force website as: “This site is hacked by Atual Dvewedi – LOG LEAVE INDIA. This is a warning message to Australian government immediately take all measures to stop resist acts against Indian students in Austrilia else I will porn all your Cyber Properties like This”.

In 2012, online phishing attacks targeted banks, e-commerce and information services, besides individuals. Jagdish Mahapatra, India Managing Director of another online security software company McAfee, forecasts a rise in targeted attacks. "2012 saw an increased growth in targeted attacks that proved successful in disrupting service and fraudulently obtaining significant amounts of intellectual property. We expect cyber criminals will continue to use this method and as a result, in 2013, we are likely to see significantly more targeted attacks and targeted malware. This type of attack is more difficult to protect against. One disturbing development in this trend across 2012 was that we started to see more targeted attacks that also destroyed evidence of the attack afterwards.

Fortinet 2013 Cybercrime Report - Cybercriminals Today Mirror Legitimate Business Processes , Cybercrime is well-established, well-equipped, and well-funded. It employs armies of employees, contractors, and partners. It constantly generates new malicious programs designed to circumvent security mechanisms, trick users into installing malware and divulging credentials and stealthily steal valuable information. However, it’s not insurmountable. As history has shown, collaborative efforts have toppled some of the world’s most powerful botnets and crime rings and will continue to do so. While new cybercrime syndicates will continue to emerge and proliferate, organizations that arm themselves with a solid, multi-layered security strategy and security best practices are doing their part in the effort to reduce the effectiveness of cybercrime.

1. **Security and role of government against the cyber crime**

The government is aware of the increasing misuse of the electronic media and online frauds. Therefore, the government of has passed the Information Technology Act 2000 to keep a track on Internet Fraud and cyber crime. The Act imposes heavy penalties and punishment on those who try to misuse this channel for personal benefit or to defraud others. The law has also established the authentication of the electronic records. Increase in the Cyber crimes in is causing cyber threat in India therefore the government has opened Cyber Crime Police Station.

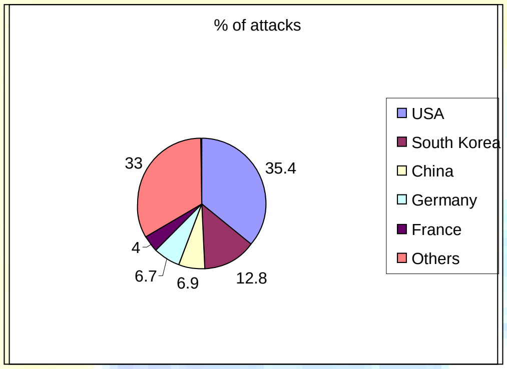
To curb cyber threat and cyber crime government has made Cyber crime cell and cyber crime police station but there is need to appoint IT and cyber security professionals. Also government has made amendments of Cyber laws and IT ACT 2000. (*Information Technology Act 2000*)

Crime Type	Description	Punishment
Tampering with Computer source documents	If there is any change in computer source documents	imprisonment up to three years/ fine up-to two lakh rupees/ both
Hacking Computer System	If computer system is hacked or any related device	imprisonment up-to three years/ up-to two lakh rupees / both
Publishing obscene information in electronic form	If any information published in electronic from and corrupt persons	imprisonment up-to five/10 years/ up-to one/ two lakh rupees / both
Penalties for misrepresentation	If misrepresentation of any data, facts, material	imprisonment up-to two years/ up-to one lakh rupees / both
Breach of confidentiality and privacy	If anybody breach the confidentiality/ privacy/ electronic record like eBook, register without permission	According to IT ACT 2000 section - 72 imprisonment up-to two years/ up-to one lakh rupees / both
Protected System	Government/ government agency has secured any computer system/network and unauthorized person hacked the security	According to Section 70 of IT ACT 2000 imprisonment up-to ten years/ liable fine / both

Source : Information Technology Act 2000

2. Impact of cyber threat on Society, IT, Government

Computer Technology and Internet can offer great benefits to the society, IT sector, organizations, nation and the whole world also. As the coin has two sides one is computer Technology and its growth another is cyber crime. This Cyber crime creats Threats to society, Government, IT Sector and may more and it disturbs entire Cyber space and creates great impact on these sectors. Cyber crime cause damage to global economics in billions dollars and many experts think that it is a promptly increasing threat for national security and social well-being. Following chart shows the percentage of top 5 cyber attacks in different countries.



Dig: Cyber attack percentage

A full-fledged cyber attack on a nation may involve three steps. first, bring down the transportation and control systems. Second, bring down the financial systems (the stock markets and banks) and third, take control of the nations' utilities. A full-scale cyber attack can cause panic among people. It can trigger alarm systems in all major establishments, be it Parliament, Rashtrapati Bhavan, major hospitals, schools or colleges. A hack into the traffic light systems can cause havoc on roads in terms of accidents. A break into the IT systems controlling the metro rail services can cause disasters. A break into your bank's system or tax department can fish out your pan number, your salary, the investments you have made, the assets you possess to the cars you own. A hack into your demat account can hurt you financially. One can know everything from details of your parents to the number of children you have. A hack into your personal computer can reveal all the searches you have made in the past to all the chat windows.

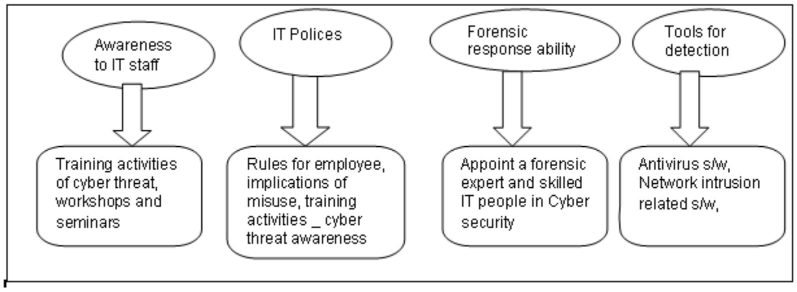
The increasing use of Internet in the business will cause the remarkable growth in business and unsafe Internet use leads into unintentional loss of confidential data as a result spying information, stealing money or merely havocking the computer, cyber criminals develop increasingly more sophisticated attack models to undermine common user practices/habits and tools. More than one-fifth of computer users now receive at least five phishing emails daily. Sometimes seen as a uncontrolled threat, phishing should instead be regarded as a potential strategic attack. The target is often a specific group of people such as a company’s customers. The targeted company’s image can be irreparably damaged while its customers can be left exposed to future victimization. Due to this fear and the insidious nature of today's threats, IT sectors placed there IT security on the ever increasing cyber threats and weakening in the direction of cyber security results in sensitive information being leaked or destroyed, financial data being stolen, all of which can severely damage a company's bottom line.[7]

III . Framework for Curbing Cyber Threat

1. AIFT MODEL for IT Sector

According to Tom Cross - X-Force Researcher, IBM Internet Security Systems ““Most people have been trained to enter social security numbers, credit card numbers, bank account numbers, etc. over the phone while interacting with voice response systems,” said Cross. “Criminals will exploit this social conditioning to perpetrate voice phishing and identity theft. At the same time, customers will demand better availability from phone service than they would from an ISP, so the threat of a DOS attack might compel carriers to pay out on a blackmail scam.”

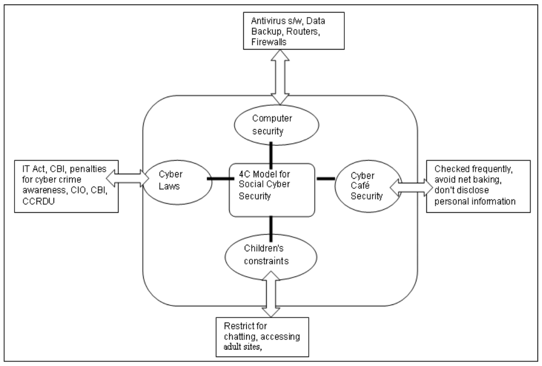
There is need to make awareness among people for cyber security and organizations too and security aware culture should be created without disturbing society, cyber cafes, and government. The skill people should be appointed for to understand the cyber crime and how to protecting computer and for avoiding the victim of threats in cyber space. The best approach for organization and staff to counter cyber crime is framework for cyber threat cyber security is represented as follows:


Awareness to IT staff
IT Polices
Forensic response ability
Tools for detection
Training activities of cyber threat, workshops and seminars
Rules for employee, implications of misuse, training activities _ cyber threat awareness
Appoint a forensic expert and skilled IT people in Cyber security
Antivirus s/w, Network intrusion related s/w,

Dig: - AIFT Model for IT sector for curbing Cyber threat

2. **Four C's for Social Security**

4 C's model for social security is as shown in the above diagram contains 4 C which structured as : C $_1$ – Computer Security, C $_2$ – Cyber Café Security, C $_3$ – Children's Constraints, C $_4$ – Cyber Laws


Antivirus s/w, Data Backup, Routers, Firewalls
Computer security
IT Act, CBI, penalties for cyber crime awareness, CIO, CBI, CCRDU
Cyber Laws
4C Model for Social Cyber Security
Cyber Café Security
Checked frequently, avoid net baking, don't disclose personal information
Children's constraints
Restrict for chatting, accessing adult sites,

Dig: Suggested 4 C's Model for Social Cyber Security

IV .Findings and Suggestions

1.

Problems to defeat the cyber crime

- Absence of Uniform Laws and National Sovereignty Related Laws : There should be uniform world wide uniform cyber laws to combat cyber crime so that the laws and their penalties should be unique everywhere. The draft amendments to IT Act 2000 do not have a single clause related to cyber terrorism or cyber war which compromises the national security, sovereignty and integrity of India.
- Lack of Awareness people are not that much aware of their rights and software copyright policy and the attitude to report the cyber crime case if any.
- Army Rights and Salary : There is need of adequate talent to intercept the communication of terrorists via the internet. The Indian Army also has professionals working on information warfare but not many individuals are keen to join them as the salary levels are very low compared to what one gets in an IT company. The basic salary of an Indian Army or Navy officer ranges between Rs 8,500 per month to Rs 26,000 per month. On the other hand, the US Navy pays its Information warfare officers salaries which start from $2000 per month (Rs 80,000) and go up to $6,300 (Rs 2.5 lakh) per month.

- Lack of Skilled People in Cyber security :Many private IT training institutes conduct courses in operating systems and ethical hacking; salaries for a fresh ethical hacker can start around Rs 4 lakh per annum. Experienced hackers just work from home and earn far higher salaries in private companies. Clearly there is a need to think of its compensation policy if it wants to attract good IT talent.
- Unsafe IT behavior : Unsafe IT behavior leads to unintentional loss of confidential information. Most of the IT people use their personal email ID for work purposes, employees feel leaking sensitive company information or infecting their company with malicious spyware or viruses puts them at greater risk of losing their job, than not adhering to their organization's Internet policy.
- Threat for online retailers :Most of the retailers did not use any external data when verifying a customer's name and address, before authorizing an online transaction. 70% of companies interviewed thought that the internet was inherently more risky than other routes to market, with the majority of respondents experiencing an increase in fraud on the Internet over the last year.

2. Suggestions

Why there is need to report the cyber crime ? When you detect something unusual or unworthy or some damage is done related to your computer network, loss of data occurs, malicious code is implemented, personal information hacked etc then you should report the Cyber crime event to secure your data and voiding to become a victim of cyber threat case. The conflict between the cyber crime and the Internet users will be there as long as the internet is there; therefore there is need to take tremendous efforts to make the awareness of Cyber threat and cyber security therefore we can motivate people to control and be aware of cyber rime and the various threats. Nothing is impossible in the world we can save our society and nation organization and strength of IT from Cyber cold War and Cyber Threat being an IT person and part of this globe. Internet is the most powerful tool for the rapid development for nation's economic and business, as well as security and sovereignty of a country therefore the cyber laws are there to punish these hackers, and the people who stole the credit cards numbers and personal information of other member's, who are creating threat, those who are spoiling or misusing the Internet and for the sake of the development of nation we have to face and solve these cyber threat problems and to minimize the frauds by creating strong security application.

Where to report and file the cyber crime case Online complaints can be filed for both cyber and Non Cyber crimes, through an online form which is available at ***http://www.bcp.gov.in/english/complaints/newcomplaint.asp*** to accept complaints filed with digital signatures. Internet Crime Compliant Center is there to file online complaint if you are the victim of Cyber crime for this refer ***https://complaint.ic3.gov/ctf.aspx*** website and you can file your case under compliant referral form IC^{3}. You can also file your compliant under CIO, the website for this is: ***http://www.cio.com/research/security/incident_response.pdf***

V. Future Directions

The cyber threat reporting to cyber crime cell so that it will help to protect and take action on cyber crime and to maintain information security and take key step ahead to curb the cyber threat from cyber space and build the superpower in the IT , Social, business sector. The cyber law covers the areas like e-governance, e-commerce, cyber contraventions and cyber offences. To curb or make awareness of cyber crime and the importance of cyber security AIFT MODEL for IT Sector and 4 'C model suggested above for social security. Also it suggest IT act and motivate people for making report or complaint of cyber crime.

VI. Conclusion

Cyberspace is common heritage for ever growing Technology all over the globe and the cyber threats are almost on the rise it is common task that all IT, organizations, countries, to be aware of threat and to make Cyber space without threat as a part of society.

It is not possible o curb 100 % cyber crime and cyber threat from cyber space but it is quite possible to make awareness among people society, organizations, and business awareness of their rights and to report cyber crime cases as a part of society. Also there is need to make some stronger cyber laws under IT Act 2000 which will provide national sovereignty and social security there is need to take proactive key steps to counter cyber threat.

VII. References

[1]CIO CYBERTHREAT RESPONSE & REPORTING GUIDELINES www.cio.com/research

[2] http://www.cyberlawtimes.com/forums/index.php?board=4.0

[3] Information Technology Act 2000 (IT ACT 2000) http://www.vishaldudeja.com/itact2000.htm

[4]www.chillibreeze.com/articles_various/Ecommerce.asp www.iamai.in A Report by eTechnology Group@IMRB for Internet and Mobile Association In India

[5]Internet Crime Complaint Center (IC3) Internet Crime Report 2008 https://complaint.ic3.gov/

[6] Sakal News Paper www.esakal.com 14 July 2009 Tuesday, page No.1

[7] Internet Fraud as One of the Cyber Threat and its Impact in India , *International Journal of Computer Science and Information Security (IJCSIS), Vol. 10, No. 11, November 2012,* **pp. 38-41** *,Ashwini Manish Brahme, Assistant Professor , Indira Institute of Management(MCA), Pune, University of Pune, Maharashtra, India*

[8] Matthews, B. (2010). Computer Crimes: Cybercrime Information, Facts and Resources. trieved from http://www.thefreeresource.com/computer-crimes-cybercrimeinformation- facts-and-resources

[9] PREVENTING CYBER CRIME: A STUDY REGARDING AWARENESS OF CYBER CRIME IN TRICITY, International Journal of Enterprise Computing and Business Systems ISSN (Online) : 2230-8849 http://www.ijecbs.com Vol. 2 Issue 1 January 2012, *Ms.Arpana , Lecturer Assistant Professor,GJIMT, Ph-II,Mohali,India Dr.Meenal Chauhan, GJIMT,Ph-II, Mohali, India*

[10] *http://www.fortinet.in/sites/default/files/whitepapers/Cybercrime_Report.pdf -* Fortinet 2013 Cybercrime Report - Cybercriminals Today Mirror Legitimate Business Processes

[11] http://businesstoday.intoday.in/story/cyber-crime-2013-online-security/1/191039.html