Gap Analysis of the Cyber Security: Challenges and the road ahead

Jatin Gupta*, Inderveer Singh*, Supriya Sharma*,

[*]Rakshak Foundation NGO

**jatingupta25@gmail.com*

**iskapriwas@gmail.com*

**ssupriya0210@gmail.com*

This research work is a comprehensive study of current scenario of cyber-crimes in India. Study is done on three fronts: firstly, the modes of cyber-attacks, the vulnerable areas, consequences of these attacks and profiles of cyber criminals; secondly, preventive measures taken by Government, private agencies or NGOs, awareness among public about these issues, solution to technical/ non-technical problems faced by government agencies like CDAC and CERT-In. Thirdly, comparative analysis of Indian and International laws on cyber terrorism, cyber censorship, pornography and jurisdictional issues harmonizing national and international legal regime. Research methodology included literature review, interviews of subject experts and surveys among Indian internet users. By these means, the data collected was used to do gap analysis in the system and recommendations were made focusing on mechanisms of awareness generation among internet users, development of a cyber-security workforce in India, including development of decentralized teams. The study suggests introduction of mandatory certification system, called `Website Security Certification System' for E-commerce websites, monitoring of ISP's to avoid misuse of internet connections on the basis of fake identities and designing of contracts with website hosts to set-up their servers within India, 'In-service' training for cyber-security professionals, to make them aware of latest threats in cyberspace. The paper also aims at studying the framework for securing critical information infrastructure achieving the same through a PPP model.

Keywords: Cyber-security,Cyber-crime,E-Commerce

1. INTRODUCTION

Cybercrime, as the name suggests includes all the crimes or offences that include use of computers or associated electronic devices. The late twentieth century, was the time when computers and the internet started gaining power and with the onset of 21st century, computers revolutionized the scene, and now it has become a necessity. Not just mails or google but from banking to shopping or social networking, with the increased use of computer, it was inevitable for its misuse to also rise rapidly. One form of this is cybercrime, which is so diverse in its nature that anyone can fall prey of it.

Computer crime can broadly be defined as criminal activity involving an information technology infrastructure, including illegal access, illegal interception, misuse of devices, forgery and electronic fraud. The World Wide Web or the cyberspace which is spread throughout the world is the place where these cybercriminals exist; they can attack any person in any corner of the world even without getting traced. Cybercrime has now become an organized activity which is valued up to US$100 billion.

These cybercriminals commit these crimes for either economic or personal motives or to cause reputational damage to somebody. In the present scenario, every person using internet is at the risk of getting affected by some sought of cybercrime. Need of the hour is to have cyber users aware of various threats and how to tackle them.

2. METHODOLOGY

2.1 Literature Survey

In this module we need to look at foreign domestic laws and international laws. A comparison between Indian and International laws can be used to study inefficiencies in Indian Laws. Study of cybercrime statistics gives an insight into the most vulnerable age group, areas of attack and most persistent cybercrimes.

2.2 Field Visits and Interviews

Conducting field visits and interviews at following institutions gives the practical feasibility of ideas proposed

- Central Bureau of Investigation,
- Intelligence Bureau,
- National Investigation Agency,
- Indian Cyber Emergency Response Team (CERT-In)

- Cybercrime Branches of Polic
- Cyber Forensics Faculty from several Training Academies

Survey regarding basic cyber security awareness was conducted among students from colleges (got 200 responses). Moreover a more diverse survey can be conducted taking into account different age groups and awareness level among them.

2.3 Expert Meetings

Expert meetings played elemental role in setting the direction for research and getting contacts of experts working in this field. Expert opinion is a must while working on issues which were revealed from field visits and needed attention and analysis. Some of the major benefits of mentor meetings were:

- Setting up agenda for the research and key areas to be focussed
- Strategy for effective implementation of recommendations proposed
- Guidance while comparing Indian Laws with International Laws
- Mechanism for Awareness Generation Model

3. RESULTS AND DISCUSSIONS

Field visits and interviews revealed a lot of things that which were not highlighted by literature analysis. Some of the key findings were:

3.1 From Public Point of View

a) **Awareness among public:** Most of the internet users are unknown of basic security measures. People often use pirated software and they are unsecured. It often seen that people have weak passwords, moreover they discloses their passwords. They easily get attracted towards fake mails about lottery's and auction without even checking the authenticity of concerned person. Very less steps are taken from prevention point of view.

b) **Unauthorised use of IP Addresses**: In India it has been seen that many government offices and universities use open proxies and does not have any security measure taken to prevent its unauthorised use. Due to this reason these IP addresses are used by unauthorised people (even by Cybercriminals) for wrong uses.

c) **Cyber Café Guidelines:** As per IT Act, 2000, any person who provides internet service must follow some guidelines and rules, but a majority of them does not follows, they don't have their own servers so that they can keep track of the websites used by the customers. This may lead to a punishment for 3 years, but no step is taken by government to keep a check on it (they only comes into effect when some incidence takes place).

3.2 From Government Point of View

a) **Unavailability of Private IP address**; Problem in tracking criminals: Most of the ISP's does not provide their customers with private IP addresses; in general they have more than 100 persons for each single public IP address. This is because while government make contracts with these companies, there was no such clause in contract. Major disadvantage is that when some person has committed some crime, then while tracking that person, it is very difficult since those 100 persons under single public IP may be distributed throughout the country and that creates a challenge to track actual criminal.

b) **Irregularity in blocking foreign country's harmful websites:** There are many websites which uses open proxies, shows obscene material and can be used to send anonymous mails. It is even harder to get data from these websites hosted in other countries, during investigation of cases. Government should take strict measures to identify and block these websites in our country. Steps must be also taken to prevent all the virtual money transactions going in cyberspace, as it is violation of FARA.

c) **Difficulty in making agreement**: India does not have a mutual agreement related to cybercrime with countries and as a result of this, if we want to get any data, we are unable to get it since most of these company's servers are in other countries. Countries like USA and China have made effective agreements in terms of cybercrime.

d) **Lack of Company's servers in India:** Many companies do not establish their servers in India, to avoid the increase in investment in our country. As a result of this, if we need any data from these websites, we need to get it from some other country hosting the server. If we don't have any ties with that country, we cannot get access to require data. The main loop hole is the contract that is initially signed with the company; it does not contain any clause for establishing their server in India. It must be noted that while making any contract with a company, a clause regarding setting up of server in our country must be present in it.

e) **Provision for CERT-In nodal branches at state level:** Steps must be taken to make CERT-In more active, this can be done by establishing nodal offices of CERT-In at state level, new recruitment for trained professionals must take place and each nodal centre must be responsible for solving regional issues and spread awareness among public, also about the misuse of their network by other people. This must be done by organising seminars and workshops at educational institutes.

f) **Lack of Knowledge at Sub-Inspector level in police:** Sub-Inspector is the first person who responds to the

complaints of people. But according to Sec. 80 of IT Act, 2000, Inspector is the lowest level of officer that will deal with issues of cybercrime and majority of inspectors and sub-inspectors don't have adequate knowledge in cybercrime, as a result of this very few cases of cybercrime gets registered. Steps must be taken to train inspectors about cybercrimes and IT Act's provisions. Even after registering cases the defence lawyer has upper stand since police officers lack proper knowledge regarding cybercrime and their legal provisions.

g) **Cyber terrorism: Anybody can be arrested:** Lack of accurate definitions of many terms viz. injury to decency and morality, may lead to life imprisonment, here decency and morality have no accurate definition. In order to stop misuse of this section 66F of IT Act, 2000, steps must be taken to elaborate upon issues of cyber terrorism.

h) **Lack of definition of abuse:** The need of the hour is to create a database of abusive terminologies after consultation with people of different places and backgrounds. For eg. word 'Chutia' is surname of people in Assam but it also an abusive word in many parts of our country, so a person sitting in US can't decide on whether it is abusive or not. Government should come forward and take actions on making decisions regarding abusive terminologies propagating on internet.

i) **Power to police**: In order to track tentative criminals and prevent subsequent crimes, police must be empowered, for eg. In order to catch criminals involved in sending obscene materials, police must be allowed to make fake social networking profiles and subsequently catching the criminals. Moreover, there must follow-up sessions for such criminals to tell the police station about their whereabouts after completion of sentence, also police can keep an eye on them.

j) **Lack of proper definition of Pornography vs. Child Pornography:** In India, it is an offence to view or transmit child pornography (involving persons below 18 years of age), but in case of adult pornography, it is illegal to transmit it but legal to view it. Government must take adequate steps to block such websites in India, make viewing adult pornography illegal and also take strict actions against people involved in this business

k) **No proper cybercrime related agreement with countries:** India have agreement with very few countries on issues of cybercrime. As in European Union countries, India must also sign treaties with countries to solve issues of international cybercrimes.

l) **Improper security measures to deliver confidential information by government:** There are lot of government websites which have inadequate security measures and confidential information can be leaked out easily. For eg. Income tax E-filing website can be used to get PAN numbers of persons by having minimal information and can be used to make fake PAN.

m) **No software development agencies in India:** In cyber forensics, some software with specific features are required and in the present scenario our government is buying these software from foreign countries that are made for their specific need, so sometimes it also goes ineffective in investigation of some cases. Government must collaborate with technical institutions in our country to develop software by taking feedback from investigation agencies. This will not only lead to effectiveness in investigation but also in reduction of expenditure.

n) **Lack of Professionals:** The present situation with Indian investigation agencies is that there are few trained professionals to combat cybercrime. Officers at higher posts (decision making positions; even in-charge of cybercrime branches) also lack necessary skills needed to tackle cybercrimes, due to this these branches does not work efficiently. It is needed to bring professional lot of people in investigation teams or there must a training program for even lowest level officer.

o) **Lack of motivation for professionals:** In the present scenario, even trained professionals have no incentives to work in government agencies since there is lot of hierarchy order in offices and in most situations higher post officers are not professional, so the work done by lower officers gets inadequate response, thus leading to demotivation.

p) **Signing Mo U's with IIT's and NIT's:** Government must come forward and sign MoU's with good technical institutes of our country, this may include development of software by their students, discussions on improving cyber security, introduction of courses on cyber security and development of good practice guidelines for general public.

3.3 From Cybercriminal Point of View

a) **Use of Multi-Proxy:** Many of the cyber criminals have started using multi proxies these days, by this they gets access to internet from an IP address in one country (say A), then opens browser by another IP address in other country (say B), then uses open proxy of a third country (say C) to send some wrong message. In these cases it is very difficult for investigators to track location of such criminals and also the legal ties between these countries are a matter of concern while investigating such cases.

3.4 Gap Analysis

a) **Lack of Professionals**: For handling cybercrime issues, persons with expertise in computer science / information technology are required. It was observed that that there is lack of trained professionals in majority of government departments handling cybercrime issues. Due to this reason, majority of cybercrimes remains unattended or unsolved. This is also a reason that very less cybercrimes gets reported (~5%). Due to this a lot of time and efforts gets wasted training these untrained professionals. Even

CERT-In is having courses for cyber auditing, people are unaware of that.

b) **No Awareness among public**: Even if government is taking appropriate measures to combat cybercrime, majority of cybercrimes takes place due to mistakes committed by public. Almost 95% of financial frauds take place due to confidential data getting leaked through phishing mails. People in different age groups uses internet for different purposes and they don't have knowledge of existing threats on internet. Good practices guidelines are not known to public. Nowadays child uses computers at very early age, and there is no cyber education for them in our education system.

c) **No Local Agencies / Teams:** All the major agencies dealing with cybercrime are situated in major cities but there are no agencies to look into cybercrimes at local level. It delays investigation of many cases and increases work load on nodal agencies at national level. Also there are many local issues like cyber café monitoring, monitoring of sale of SIM cards and control over unsecured open proxies cannot be done unless there are local agencies.

d) **Irresponsible Functioning of ISP's:** At present ISP's does not take any steps to filter harmful / improper content on internet. Moreover, sale of SIM cards is done in unaccountable manner and due to this in many cybercrime cases fake SIM cards are used. When ISP's are asked to provide logs / data during investigation process, they provide them in unorganized manner without any specific format, which leads to excess wastage of time and efforts in order to sort out these logs.

e) **Problems in Coordination between Public and Law Enforcement agencies:** In IT Act, inspector is lowest level officer to register any FIR under IT Act but at majority of police stations Sub-Inspectors are responsible for registering FIR's. This leads to lack of coordination between victim and police. Moreover, senior officers at these police stations have less knowledge about cybercrimes and IT Act, thus many cases of cybercrime does not gets registered.

f) **Excessive Work Pressure on Forensic Labs (FSL's):** At present there are very less forensic labs in our country and during investigation of most of cybercrime cases FSL's needs to do evidence analysis. With increase in number of cybercrimes, it is becoming very difficult for FSL's to handle all the cases effectively and investigate them accurately.

g) **Improper Transfer policies for Cybercrime branches:** It is observed that in most of Cybercrime Branches, officers who have either very less or no knowledge of information technology are getting transferred. It takes them additional efforts to get trained in this field. This generally leads to reduction in proper functioning of these branches. Also trained professionals are transferred in normal police stations thus leading to decrease in cyber security workforce. This leads to gradual demotivation of professionals. It is necessary to have specialised policies for cybercrime branches so that professionals goes to correct place.

h) **Lack of Courses on Cyber Security in Technical Institutions:** Very few Technical Institutions in India have courses on cyber security or forensics. As a result of this, students are unknown to this aspect of their studies. Due to reduced number of trained professionals in this field, there is a lack of good quality software related to cyber forensics; moreover, most of the software currently in use for this purpose is imported from other countries. They lack efficiency in our country since they are made for that country's specific purpose.

i) **Loopholes in IT Act:** In the amendment act, positive steps have been taken by government to make the Law more effective by bringing in idea of electronic signature rather than digital signature. Even after this proactive attempt by government, there are some sectors in Act which needs further analysis, these are:

j) **Child Pornography:** Though this section has been drafted with some care but still some intricacies are not well addressed. It talks only of sexualized representations of actual children, and does not include fantasy play-acting by adults, etc. From a plain reading of the section, it is unclear whether drawings depicting children will also be deemed an offence under the section. Regarding the age of differentiating a child from an adult, it has been mentioned that 18 years is the limiting age but in section 67B age of children is being defined as older than the age of sexual consent. This needs to be reframed.

k) **Transmission of obscene material online:** In sec 67, 67A and 67B, the phrase "Causes to be transmitted" is used. It would mean that the producer, the recipient and the the person from whose server the data has been sent will all be charged for it. Steps need to be taken to strengthen it and this can act as a cap on transmission of obscene material online.

l) **Offensive Messages (Section 66A):** There needs to be a strict definition for type of offensive material. The fact that some information is "grossly offensive" or it causes "annoyance" or "inconvenience" while being known to be false cannot be applied to everything. But issues related to decency, morality, public order or defamation must be handled carefully under this section.

m) **Blocking of Websites:** There is no specific guidelines or process regarding blocking of websites. Any material available on internet that is harmful to public (or person in specific) is liable to be blocked by government. But in order to tackle the issues of internet censorship, there must be some governing board or team that must look into details of blocking websites.

n) **No provision for monitoring of E-Commerce Websites:** IT Act does not have any section regarding certification mechanism for websites having monetary transactions online. Moreover there isn't any provision regarding the minimum necessary security measures that needs to be incorporated by these websites.

o) **Cyber Terrorism:** Section 66F (1)(B), defining "cyber terrorism" is much too wide, and includes unauthorised access to information on a computer with a belief that that information may be used to cause injury to decency or morality or defamation, even. While there is no one globally accepted definition of cyber terrorism, it is tough to conceive of slander as a terrorist activity.

p) **Penalties:** Most of cases having offences carrying penalties above three years imprisonment have been made cognizable, they have also been made bailable and lesser offences have been made compoundable. This is a desirable amendment, especially given the very realistic possibility of incorrect imprisonments (Airtel case, for instance), and frivolous cases that are being registered (Orkut obscenity cases). There must be more analysis on which offences must be made non-bailable and rest bailable.

q) **Cheating by personation:** It is not clear whether it refers to cheating as referred to under the Indian Penal Code as conducted by communication devices, or whether it is creating a new category of offence. In the latter case, it is not at all clear whether a restricted meaning will be given to those words by the court such that only cases of phishing are penalised, or whether other forms of anonymous communications or other kinds of disputes in virtual worlds (like Second Life) will be brought under the meaning of "personation" and "cheating".

Some of these issues have been addressed in National Cyber Security Policy, 2013, but main hurdle lies in successful implementation of changes proposed.

4. CONCLUSIONS AND RECOMMENDATIONS

4.1 Awareness Generation Mechanism

During literature analysis, field visits and surveys conducted, it is observed that there is a need to generate awareness on cyber security issues, since 70% of all cybercrimes take place due to some mistake done by victim. Since majority of victims of cybercrimes are youth between age of 18-30 years, so we need to specifically target population in this age group and the ones entering into it in near future.

4.2 Certification of E-Commerce Websites

All the E-Commerce websites must undergo a mandatory certification process to conduct cyber security audit of their website so as to accredit their website. This cyber security audit will give the website owner information about various vulnerabilities on website and will be rated accordingly. So in order to attract crowd on its website, they need to improve their security measures and improve their rating. Thus having improved security measures for these websites.

4.3 Monitoring of ISPs

All the ISP's must have strict provision on sale of SIM cards. In order to avoid misuse of credentials of customers by local vendors, there must be a strong checking mechanism to be implemented by these ISP's. Now, how to force ISP's to implement such policy, in IT Act, a clause must be added in which ISP's must also be made responsible for any crimes committed by their network. ISP's must be instructed to block those websites that are notified by respective authorities to be harmful.

4.4 Amendments in IT Act

a) **Cyber Terrorism (Sec. 66F):** Its scope must be limited down to cyber activities that create panic among large population or lead to mass destruction. Moreover, terms like decency / morality must be more precisely used with their proper application.

b) **Child Pornography (Sec. 67B):** In this section, stress is laid on word child and that on the age below 18 years. In this section various forms of pornography must be included that may involve computer graphics involving children or adults imitating a child and making porn. Moreover, transmitting and viewing child pornography is a crime; similar conditions must also be put on adult pornography. A clause must be added in which ISP's must also be made responsible for any crimes committed by their network and they must be instructed to block / filter such contents.

c) **Blocking Illicit Content (Sec. 69A):** This section must be strengthened to block any illicit content and this must be done by ISP's. In order to tackle the issues of internet censorship, specific guidelines for blocking of websites / content must be made. Moreover, a committee must be formed and they must analyse the parameters for such instructions to ISP's.

d) **Mandatory Certification of E-Commerce Websites:** A section must be included that takes into account the security measures taken by E-Commerce websites and that must be insured by mandatory certification and rating these websites based on the level of security (This may be similar to star rating of electrical appliances).

REFERENCES

1. IT Act, 2000 and IT (Amendment) Act, 2008
2. National Cyber Security Policy, July 2013
3. Crime in India, National Crime Records Bureau, Statistics for year 2012
4. Data Security Council of India (DSCI) (http://www.dsci.in/)
5. Indian penal Code (IPC) for basic crimes that also fall in domain of IT Act

6. Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL)
7. European Convention on Cybercrime
8. United Nations Office on Drugs and Crime (UNODC) Comprehensive Study on Cybercrime, Draft, February, 2013
9. Justice S. B. Sinha, "*Cyber Crime in the Information Age*", Cyber Space and The Law – Issues and Challenges, NALSAR University, 2004
10. Cyber Crime and its Jurisdiction in India, by Abhay Pratap Singh and Pranay Bagdi
11. UNCITRAL and European Convention on Cybercrime
12. Comprehensive Study on Cybercrime, UNODC, 2013
13. Sophos Security threat Report 2013
14. Fortinet 2013 Cybercrime Report
15. 2012 Cost of Cybercrime Study: United States, by Ponemon Institute
16. RSA 2012 Cybercrime Trends Report
17. Short Note on IT Amendment Act, Pranesh Prakash, http://cis-india.org/internet-governance/publications/it-act/short-note-on-amendment-act-2008
18. Information Security Awareness CDAC
19. CERT-In Website, http://www.cert-in.org.in/
20. http://www.first.org/resources/guides
21. Satheesh G Nair's Blog on Cybercrime, For case studies,
22. Cyber Law Consulting, for case studies, http://www.cyberlawconsulting.com/cyber-cases.html
23. Present trends of Cybercrime, http://www.go-gulf.com/blog/cyber-crime/