November 2015 IJMIE Volume 5, Issue 11 ISSN: 2249-0558

# A STUDY OF CYBER SECURITY ISSUES AND CHALLENGES ON LATEST TECHNOLOGIES IN INDIA

S. K. Nayak[*]

Dr. C. S. Panda[**]

## ABSTRACT

If cyber security was easily addressed we wouldn't be writing this white paper. The reality is that there are no easy or perfect answers to this challenge. Cyber security as an issue is too broad, there are too many devices being connected to the internet that have variable security, too many vulnerabilities in hardware and software, the rate of change in technology is too great, and actors with ill intent only need to be successful once while defenders of cyber security have to be successful all of the time. Cyber Security plays an important role in the field of information technology. Securing the information has become one of the biggest challenges in the present day. Whenever we think about the cyber security the first thing that comes to our mind is **'cyber crimes'** which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cyber crimes. Besides various measures, cyber security is still a very big concern to many. This paper presents introduction to cyber security and the various threats to the cyber security and how these threats can be resolved. This paper mainly focuses on challenges faced by cyber security issues and challenges on the latest technologies in India. To resolve issues related to cyber security the community of security researchers- including academia, the private sector and government sector must work together to understand the emerging threats to the computing world.

**Keywords:** cyber security, cyber crime, Aspects, Challenges, National Security Policy.

## 1. INTRODUCTION

[*] M.Phil Student, PG. Dept. of Comp. Sc. and Applications, Sambalpur University, Odisha, India

[**] Lecturer, PG. Dept. of Comp. Sc. and Applications, Sambalpur University, Odisha, India

Cyber Security is of major concern in today's era of computing to secure data, network resources, and other critical information of an organization. Cyber security is now not restricted only to usage of Internet on a Desktop PC but securing information on Tablets, smart phones as they became very important communication medium because of technological advancements grown up very rapidly in past few years[1].

Today man is able to send and receive any form of data may be an e-mail or an audio or video just by the click of a button but did he ever think how securely his data id being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today Internet is the fastest growing infrastructure in everyday life. In today's technical environment many latest technologies are changing the face of the mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cyber crimes are increasing day by day. Today more than 60 percent of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. Hence cyber security has become a latest issue. The scope of cyber security is not just limited to securing the information in IT industry but also to various other fields like cyber space etc.

Even the latest technologies like cloud computing, mobile computing, E-commerce, net banking etc also needs high level of security. Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cyber crime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber crime effectively. Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Every individual must also be trained on this cyber security and save themselves from these increasing cyber crimes [2].

## 2. CYBER CRIME

Cyber crime is a term for any illegal activity that uses a computer as its primary means of commission and theft. The U.S. Department of Justice expands the definition of cyber crime to include any illegal activity that uses a computer for the storage of evidence. The growing list of cyber crimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major problem to people and nations. Usually in common man's language cyber crime may be defined as crime committed using a computer and the internet to steel a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs. As day by day technology is playing in major role in a person's life the cyber crimes also will increase along with the technological advances.

## 3. CATEGORIES OF CYBER CRIME

**3.1 Hacking:** Hackers make use of the weaknesses and loop holes in operating systems to destroy data and steal important information from victim's computer. It is normally done through the use of a backdoor program installed on your machine. A lot of hackers also try to gain access to resources through the use of password hacking software. Hackers can also monitor what u do on your computer and can also import files on your computer. A hacker could install several programs on to your system without your knowledge. Such programs could also be used to steal personal information such as passwords and credit card information. Important data of a company can also be hacked to get the secret information of the future plans of the company.

**3.2 Cyber-Theft:** Cyber-Theft is the use of computers and communication systems to steal information in electronic format. Hackers crack into the systems of banks and transfer money into their own bank accounts. This is a major concern, as larger amounts of money can be stolen and illegally transferred. Credit card fraud is also very common. Most of the companies and banks don't reveal that they have been the victims of cyber -theft because of the fear of losing customers and shareholders. Cyber-theft is the most common and the most reported of all cyber-crimes. Cyber- theft is a popular cyber-crime because it can quickly bring experienced cyber- criminal large cash resulting from very little effort

**3.3 Viruses and worms:** These are the very major threat to normal users and companies.

Viruses are computer programs that are designed to damage computers. It is named virus because it spreads from one computer to another like a biological virus. A virus must be attached to some other program or documents through which it enters the computer. A worm usually exploits loop holes in software or the operating system. Trojan horse is dicey. It appears to do one thing but does something else. The system may accept it as one thing. Upon execution, it may release a virus, worm or logic bomb. A logic bomb is an attack triggered by an event, like computer clock reaching a certain date.

**3.4 Spamming:** It involves mass amounts of email being sent in order to promote and advertise products and websites. Email spam is becoming a serious issue amongst businesses, due to the cost overhead it causes not only in regards to bandwidth consumption but also to the amount of time spent downloading/ eliminating spam mail. Spammers are also devising increasingly advanced techniques to avoid spam filters, such as permutation of the emails contents and use of imagery that cannot be detected by spam filters.

**3.5 Financial Fraud:** These are commonly called “Phishing’ scams, and involve a level of social engineering as they require the perpetrators to pose as a trustworthy representative of an organization, commonly the victim’s bank.

**3.6 Identity Theft, Credit Card Theft, Fraudulent Electronic Mails (Phishing):** Phishing is an act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in order to scam the user into surrendering private information that will be used for identity theft.

**3.7 Cyber harassment:** It is an electronically and intentionally carrying out threatening acts against individuals. Such acts include cyber-stalking.

**3.8 Cyber laundering:** It is an electronic transfer of illegally-obtained monies with the goal of hiding its source and possibly its destination.

**3.9 Website Cloning:** One recent trend in cyber-crime is the emergence of fake ‘copy-cat’ web sites that take advantage of consumers what are unfamiliar with the Internet or who do not know the exact web address of the legitimate company that they wish to visit. The consumer, believing that they are entering credit details in order to purchase goods from the intended company, is instead unwittingly entering details into a fraudster’s personal database. The fraudster is then able to make use of this information at a later stage, either for his own purposes or to sell on to others interested in perpetrating credit card fraud [3, 4].

## 4. ASPECTS OF CYBER CRIMES

### 4.1 Technological Aspect of Cybercrime

From a technological dimension, other experts point out the need for a comprehensive term, such as *"electronic crime"* or *"e-crime"*, thanks to the convergence of ICT, including mobile technology, telephony, memory, surveillance systems, and other technologies, including nanotechnology and robotics, which must be taken into account from now on. These electronic media will be targeted increasingly more often and will also be used to conceal, commit, or support crimes and offenses. Only the positive actions for which one or more means were used to commit one of the elements of the offense can be included.

### 4.2 Anthropological Aspect of Cybercrime

From an anthropological aspect, cybercrime originates from various populations and exhibits socio- educational, socio-economic, and techno-ideological factors and their expressions, including pathological expressions like addiction. The maladjustment of the education system may contribute to the development of new forms of cybercrime or deviant practices and behavior with various levels of severity, including cheating and reputational damage, which can be related to frustrations and the redefinition of material and citizen values, inconsistent with what is expected when approaching and leading an adult life. Difficult socio- economic conditions also include the Internet as a place for expressing psychological troubles with socio-economic origins, including theft, child pornography, and calls for uprisings, violence, and hatred. With regard to techno- ideological factors, one must consider sites and networks aimed at propaganda, destabilization, and individual and mass psychological manipulation using methods that involve the digital processing of images, videos, and audio.

### 4.3 Strategic Aspect of Cybercrime

From a strategic aspect, cybercrime is seen as an offense to cyber-security, namely attacks to digital networks for the purpose of seizing control, paralyzing them, or even destroying infrastructures that are vital to governments and sectors of vital importance [5].

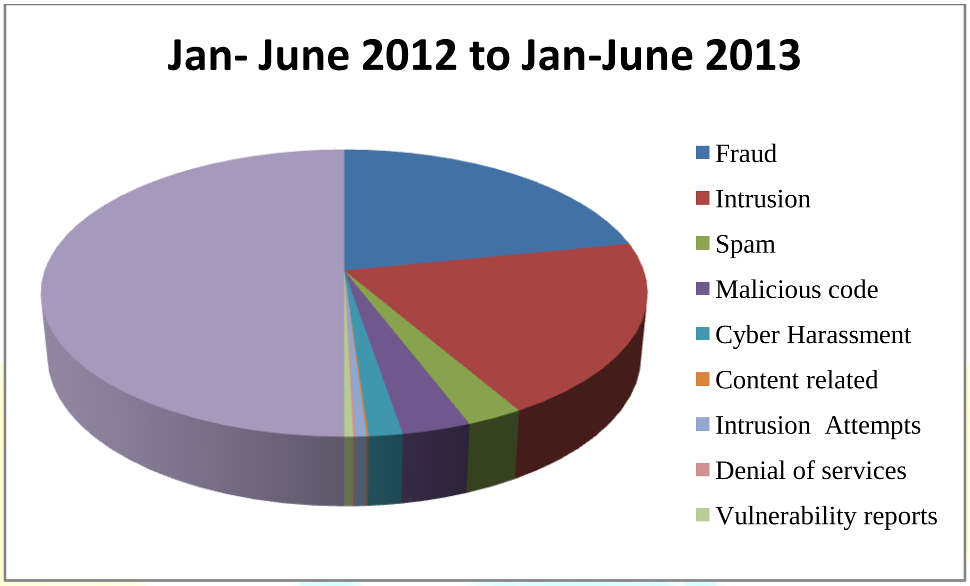
## 5. CYBER SECURITY

Privacy and security of the data will always be top security measures that any organization takes care. We are presently living in a world where all the information is maintained in a digital or a cyber form. Social networking sites provide a space where users feel safe as they interact with friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during bank transactions a person must take all the required security measures.

(Table-1)

| Incidents | Jan- June 2012 | Jan- June 2013 | % Increase/ (decrease) |
|---|---|---|---|
| Fraud | 2439 | 2490 | 2 |
| Intrusion | 2203 | 1726 | (22) |
| Spam | 291 | 614 | 111 |
| Malicious code | 353 | 442 | 25 |
| Cyber Harassment | 173 | 233 | 35 |
| Content related | 10 | 42 | 320 |
| Intrusion Attempts | 55 | 24 | (56) |
| Denial of services | 12 | 10 | (17) |
| Vulnerability reports | 45 | 11 | (76) |
| Total | 5581 | 5592 | |

(Source: http://www.arxiv.org/ftp/arxiv/papers/1402/1402.1842.pdf)



(Fig.-1)

The above Comparison of Cyber Security Incidents reported to Cyber999 in Malaysia from January–June 2012 and 2013 clearly exhibits the cyber security threats. As crime is increasing even the security measures are also increasing. According to the survey of U.S. technology and healthcare executives nationwide, Silicon Valley Bank found that companies believe cyber attacks are a serious threat to both their data and their business continuity.

- 98% of companies are maintaining or increasing their cyber security resources and of those, half are increasing resources devoted to online attacks this year
- The majority of companies are preparing for when, not if, cyber attacks occur
- Only one-third are completely confident in the security of their information and even less confident about the security measures of their business partners.

There will be new attacks on Android operating system based devices, but it will not be on massive scale. The fact tablets share the same operating system as smart phones means they will be soon targeted by the same malware as those platforms. The number of malware specimens for Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications for virtually any device (PCs, tablets and smart phones) running Windows 8, so it will be possible to develop malicious applications like those for Android, hence these are some of the predicted trends in cyber security.

## 6. CHALLENGES TO INDIA'S NATIONAL CYBER SECURITY ON LATEST TECHNOLOGY

The Cyber Law Trends and Developments of India 2013 has already been covered by Perry4Law and Perry4Law's Techno Legal Base (PTLB)[6].

**(i) National Cyber Security Policy India:** Cyber Security in India has been ignored for long. However, Indian Government realized that this is a crucial field and it needs a clear Cyber Security Policy. The National Cyber Security Policy of India 2013 (NCSP 2013) was drafted keeping this requirement in mind. It is a good Policy on many counts but it also failed to address many crucial aspects as well. For instance, the Policy has failed to protect Privacy Rights in India. Nevertheless, this is a good step in the right direction and it must be updated and improved as the time passes

**(ii) National Security Policy Of India:** National Security of India is facing many challenges these days that are mainly attributable to the use and abuse of Information and Communication Technology (ICT).A National Security Policy of India is urgently needed that must have the Cyber Security Policy as an essential element. Presently this is not the case but we hope the same would be achieved very soon by the Indian Government.

**(iii) National Telecom Security Policy of India:** There is no implementable National Telecom Security Policy of India as on date. However, it may be drafted very soon by the Indian Government. As of now the Telecom Service Providers of India are openly flouting the Laws of India. They are not following the Cyber Law Due Diligence in India. For instance, Airtel and Tata Teleservices Limited are violating Cyber Law of India in general and Internet Intermediary Rules of India in particular. These violations must be punished by Department of Telecommunication (DoT) and Telecom Regulatory Authority of India (TRAI). Even the Defence Research and Development Organisation (DRDO) has communicated to the DoT that the proposed National Telecom Security Policy should have a framework to penalize Telecom Service Providers if they fail to abide by the norms.

**(iv) Imported Software and Telecom Equipments Security:** Cyber Security of imported Software and Telecom Products was a major cause of concern for India. For instance, Huawei and ZTE have already faced Telecom Security Issues in India. Similarly, India is also considering making the Norms for import of Telecom Equipments in India more stringent. The Security Agencies of India have gone to the extent of even suggesting for the developing indigenously manufactured Cyber Security Software. Although the testing of Imported Software and Hardware for embedded Malware has been postponed till 1st April 2014 by India yet this issue would resurface in the year 2014. Even a Telecom Security Directorate of India has been proposed by Indian Government.

**(v) Cyber Security of E-Governance:** Cyber Security of E-Governance Services in India is still not upto the mark. The Cyber Security in India must be improved so That Public Services can be better delivered through the mode of E-Governance and Mobile Governance. Similarly, Cyber Security Legal Practice must be encouraged and developed in India so that Cyber Crimes and Cyber Security related breaches can be properly prosecuted.

**(vi) E-Mail Policy of India:** There has been an increase in the use of Private E-Mails for committing Cyber Crimes in India and worldwide. For instance, E-Mail Service Providers like G-mail are abetting and encouraging commission of Cyber Crimes. E-Mail Service Providers like G-Mail, Yahoo, Hotmail, etc are also facilitating violating the provisions of Public Records Act, 1993 wherever public Records are involved and they must be banned in India. Realising the seriousness of the situation, Delhi High Court is analyzing E-Mail Policy of India and complaint mechanism to Facebook. The Delhi High Court has also directed Central Government to Issue Notification regarding Electronic Signature under Information Technology Act 2000. An advisory by Maharashtra Government to use official E-Mails has already been issued. Even the E-Mail Policy of India has been proposed by Indian Government.

**(vii) Cyber Security of Private Banks in India:** Cyber Security of Banks in India is still not taken seriously. Banks are not interested in ensuring Cyber Security of electronic transactions. The Recommendations of Reserve Bank of India (RBI) to ensure Cyber Security, appointment of Chief Information Officers (CIOs), establishing a Steering Committee at board level, etc has remained unfulfilled. Even RBI has warned banks for inadequate Cyber Security. If the online business or transaction pertains to Banking Industry, especially online transfer and receiving of money, the applicable provisions can include the Internet Banking Guidelines, Mobile Banking Security Practices, e-Commerce Regulations and Compliances, Risk Management for Card Present Transactions, etc.

**(viii) Mobile Payment Cyber Security:** Mobile Security in India is still a serious concern in India. The truth is that India is Not Ready for Mobile Governance as on date. Mobile Banking

Cyber Security in India is still missing and the same must be established on a priority basis. Incidences of ATM Frauds, Credit Card Frauds, Phishing, RTGS Frauds, Internet Banking Frauds, etc have increased significantly in India. Malware targeting mobiles specifically have also raised the threat level further. On top of it we have poor adoption cyber security practices and policies by banks of India. In short, the Online Banking System of India is Not Cyber Secure and Mobile Payments Cyber Security in India is needed especially when the RBI is suggesting use of SMS Based Funds Transfer in India.

**(ix) Cyber Security Capabilities:** Incidences of Cyber Crimes, Cyber Attacks, Cyber Security Incidences, Cyber Warfare, Cyber Terrorism, Cyber Espionage, etc are some of the problems that are peculiar to the contemporary times. These threats are intimidating the National Security of India by striking at the Financial, Economic, Social and Political Environment of India. Offensive and Defensive Cyber Security Capabilities of India is need of the hour. Even the National Cyber Security Policy of India 2013 (NCSP 2013) recognized this fact. Techno Legal Skills Development in India is need of the hour and India must stress more upon Online Skills Development and E-Learning Methods to fill this skills gap.

**(x) Cyber Security Legal Practice:** Cyber Security Legal Practice is the emerging Global Trend. Naturally, Cyber Security Legal Practice in India is still maturing. More and more Law Firms and Lawyers need to take up Cyber Security as a Legal Practice in India.

**(xi) Cyber Security Awareness In India:** Cyber Security Awareness in India is required to be enhanced. Keeping this in mind, the Cyber Security Awareness Brochures were mooted in India by Indian Government. Now Computer Hardware Providers in India are required to mandatorily provide Cyber Security Awareness Brochures along with their Products.

**(xii) Cyber Security Disclosure Norms In India:** The Cyber Security Infrastructure in India is struggling hard to catch up the Malware ridden Internet and growing Cyber Attacks against India. As there is no requirement to inform about a Cyber Security Breach and Cyber Security Incidence, no private company or institution in India is reporting such crucial Cyber Security Incidences. To tackle this situation, the Indian Government is planning a Legislation Mandating Strict Cyber Security Disclosure Norms in India. This is a good step in the right direction provided the Indian Government actually implements what it has suggested.

## 7. CONCLUSION AND RECOMMENDATIONS

As the general population becomes increasingly refined in their understanding and use of computers and as the technologies associated with computing become more powerful, there is a strong possibility that cyber-crimes will become more common. India is rated as one of the countries with the highest levels of e-crime activities. Cyber security must be addressed seriously as it is affecting the image of the country in the outside world. Information attacks can be launched by anyone, from anywhere. The attackers can operate without detection for years and can remain hidden from any counter measures". This indeed emphasizes the need for the government security agencies to note that there is need to keep up with technological and security advancements. There is need to create a security-aware culture involving the public, the ISPs, cybercafés, government, security agencies and internet users. Also in terms of strategy, it is crucial to thoroughly address issues relating to enforcement. Mishandling of enforcement can backfire.

## References

[1] A.K.Verma, A.K. Sharma, Cyber Security Issues and Recommendations, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 4, April 2014.

[2] G.Nikhita Reddy, G.J. Ugander Reddy, A Study of Cyber Security Challenges and its Emerging Trends on Latest Technologies, http://www.arxiv.org/ftp/arxiv/papers/1402/1402.1842.pdf

[3] Strassmann, P.A. (2009) Cyber Security for the Department of Defence Retrived July 10, 2011 From http://www.strassmann.com/pubs/dod/cybersecurity-draft-v1.pdf

[4] Oliver, E. O. (2010): Being Lecture Delivered at DBI/George Mason University Conferenceon Cyber Security holding, Department of Information Management Technology Federal University of Technology, Owerri, 1-2 Nov.

[5] Yougal Joshi, Anand Singh, A Study on Cyber Crime and Security Scenario in INDIA, International Journal of Engineering and Management Research, Vol.-3, Issue-3, pp.13-18,June 2013

[6] Perry4Law An Exclusive Techno-Legal Corporate, IP & ICT Law Firm, New Delhi, India, Cyber Security Trends And Developments In India[online] available: http://www.perry4law.com/, http://www.ptlb.in/, http://www.perry4law.org/