International Journal of Engineering Research & Management Technology
ISSN: 2348-4039
May-2018 Volume 5, Issue-3
Email: editor@ijermt.org
www.ijermt.org

IMPORTANCE OF CYBER SECURITY IN INDIA

Alok Kumar Gupta
Research Scholar
Noida International University
Greater Noida

Dr. Mayank Singh
Supervisor
Noida International University
Greater Noida

ABSTRACT
The Cyber Security Market in Asia Pacific, which stood at USD 17 Bln in 2015, is poised to grow at a CAGR of 12.3%, reaching USD 54 Bln by the year 2025. According to industry estimates, the increasing incidents of cyber-attacks and data protection efforts globally, would create USD 35 Bln revenue opportunity and would provide employment for about a million professionals in India by 2025. However, to capitalize on these opportunities, the Indian Cyber Security industry has to overcome the challenges it faces, and has to come up with a clear and organized agenda, which would involve, inter alia, strong Cyber Security policy and regulation, focus on capacity building both at government and industry levels, developing new products through R&D collaborations, supply of new products and services and cyber forensics. The paper details about the nature of cyberspace and shows how the internet is unsecure to transmit the confidential and financial information. We demonstrate that hacking is now common and harmful for global economy and security and presented the various methods of cyber attacks in India and worldwide.

Keywords
Cyber security, government and industry

INTRODUCTION
Cyber security is defined as technologies and processes constructed to protect computers, computer hardware, software, networks and data from unauthorized access, vulnerabilities supplied through Internet by cyber criminals, terrorist groups and hackers. Cyber security is related to protecting your internet and network based digital equipments and information from unauthorized access and alteration. Internet is now not only the source of information but also has established as a medium through which we do business, to advertise and sell our products in various forms, communicate with our customers and retailers and do our financial transactions. The internet offers lots of benefits and provides us opportunity to advertise our business across the globe in minimum charges and in less human efforts in very short span of time. As internet was never constructed to track and trace the behavior of users. The Internet was actually constructed to link autonomous computers for resource sharing and to provide a common platform to community of researchers. As internet offers on the one hand huge number of benefits and on the other hand it also provides equal opportunities for cyber-terrorists and hackers. Terrorist organizations and their supporters are using internet for a wide range of purposes such as gathering information and dissemination of it for terrorist purpose, recruiting fresh terrorists, funding attacks and to motivate acts of terrorism. It is often used to facilitate communication within terrorist groups and gathering and dissemination of information for terrorist purposes.

WHAT IS CYBER SECURITY?
The dictionary meaning says that Cyber Security is state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this. It is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing

devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

Cyber security ensures the maintenance of the security properties of the organization and user's assets against security risks in the networked environments. It is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. Elements of cyber security include:

Application security which is the use of software, hardware, and procedural methods to protect applications from external threats.

- Information security is the practice of avoiding information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. IT Security and Information assurance are two major aspects of information security.
- Network security which consists of the provisions and policies adopted by a network administrator. They prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals.
- Disaster recovery / business continuity planning - need to encompass how employees will communicate, where they will go and how they will keep doing their jobs. The details can vary greatly, depending on the size and scope of a company and the way it does business. For some businesses, issues such as supply chain logistics are most crucial and are the focus on the plan. For others, information technology may play a more pivotal role, and the BC/DR plan may have more of a focus on systems recovery. For example, the plan at one global manufacturing company would restore critical mainframes with vital data at a backup site within four to six days of a disruptive event, obtain a mobile PBX unit with 3,000 telephones within two days, recover the company's 1,000-plus LANs in order of business need, and set up a temporary call center for 100 agents at a nearby training facility.
- End-user education involves educating end users with various information attacks and how to avoid them. For example, while registering password, tell end user what should be the length and characteristics of complex password. Provide suitable education about what are the precautions they have to take to avoid cyber crimes. Also, sometimes actions to be taken in case if they are victim.

OTHER INDIAN GOVERNMENT INITIATIVES

Indian government released National Cyber Security Policy on July 2, 2013. This policy addressing the growth of information technology, increasing number of cyber crimes, plans for social transformation. It has 14 objectives which includes enhancing the protection of India's Critical infrastructure to investigation and prosecution of cyber crime, developing 50,000 skilled cyber security professionals in next five years:

- **Cyber Security Research And Development Centre Of India (CSRDCI)** –
  This concentrates on Techno Legal Cyber Security Issues of India and World Wide]. This Platform and Website is managed by Perry4Law, Perry4Law Techno Legal Base (PTLB) and Perry4Law Techno Legal ICT Training Centre (PTLITC). the Cyber Security Initiatives and Projects of PTLB at a single place.

- **Cyber Crimes Investigation Centre Of India –**
  The Cyber Crime Investigation Centre of India (CCICI) is the exclusive Techno Legal Cyber and Hi-Tech Crimes Investigation and Training Centre (CHCIT) of India. The objective of CCICI is to spread Cyber Law Awareness and Cyber Security Awareness in India and abroad. Further, CCICI also intends to develop Cyber Crimes Investigation Capabilities and Expertise in India and abroad.

- **National Intelligence Grid (NATGRID)** –
  This Project of India is one of the most ambitious Intelligence Gathering Project of India. It has been launched at a time when the Intelligence Infrastructure of India is in a bad shape. It is an essential requirement for robust and effective Intelligence Agencies and Law Enforcement functions in India.

- **National Critical Information Infrastructure Protection Centre (NCIPC) Of India** - intends to ensure critical infrastructure protection and critical ICT infrastructure protection in India.
- **National Cyber Security Database of India (NCSDI)** -
  This Database would work in the direction of fighting against Cyber Threats and Cyber Attacks including Cyber Terrorism Against India, Cyber Warfare Against India, Cyber Espionage Against India, Critical Infrastructure Protection in India, Managing India's Cyber Security Problems, Issues and Challenges, etc.

CHALLENGES IN CYBER SECURITY

- Cyber security has been considered as one of the most urgent national security problems. A report says, in a speech during his presidential campaign, President Obama promised to "make cyber security the top priority that it should be in the 21st century . . . and appoint a National Cyber Advisor who will report directly" to the President.
- Cyber security must address not only deliberate attacks, such as from disgruntled employees, industrial espionage, and terrorists, but inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize a network in unpredictable ways.
- The defense of cyberspace necessarily involves the forging of effective partnerships between the public organizations charged with ensuring the security of cyberspace and those who manage the use of this space by myriad users like government departments, banks, infrastructure, manufacturing and service enterprises and individual citizens. The defense of cyberspace has a special feature. The national territory or space that is being defended by the land, sea and air forces is well defined. Outer space and cyberspace are different. They are inherently international even from the perspective of national interest.

NEED FOR CYBER SECURITY IN INDIA

9.4% houses in India have computer (any of Laptop or Desktop). Chandigarh (U/T), Goa and NCT of Delhi are top three stats/union territories with highest computer usage. According to 2018 Census, Only 2.3 percent of total houses have Internet access in India. The census covered 34,66,92,667(346.7 million) houses in India and found only 86,47,473 (3.3%) of this houses use Internet. The Internet includes both broadband and low-speed connections.

INDIA'S LEGAL FRAMEWORK FOR CYBER SECURITY

1. **Indian IT Act, 2000 :** Section 65 - Tampering with computer source code, Section 66 - Hacking & computer offences, Section 43 – Tampering of electronic records

2. **Indian Copyright Act:** States any person who knowingly makes use of an illegal copy of computer program shall be punishable. Computer programs have copy right protection, but no patent protection.
3. **Indian Penal Code:** Section 406 - Punishment for criminal breach of trust and Section 420 - Cheating and dishonestly inducing delivery of property.
4. **Indian Contract Act, 1872 :** Offers following remedies in case of breach of contract, Damages and Specific performance of the contract

INDIAN GOVERNMENT INITIATIVES FOR EDUCATION ON CYBER SECURITY

Information security awareness – This is launched from over a five years period. One of the objectives is to create awareness about information security to children, home users and non-IT professionals in a systematic way. C-DAC Hyderabad has been assigned this project.

Information security education and awareness project- Objectives are to train System Administrators by offering Diploma Course in Information Security, Certificate Course in Information Security, 6-weeks/2-weeks training programme in Information Security, train Government Officers of Center and State on Information Security issues and Education Exchange Programme

National Initiative for Cybersecurity Education (NICE) - The goal of NICE is to establish an operational, sustainable and continually improving cyber security education program for the nation to use sound cyber practices that will enhance the nation's security.

INTERNET USAGE IN INDIA

India has experienced tremendous growth of information technology and established itself as popular IT destination in world. It is ranked on number three position in world after China and United State in the usage of internet. A report from IAMAI revels that India is expected to be second largest by 2015 with 330 to 370 million internet users.

More than 200 million users started to use internet after 2010. The total number of internet users were 306 million in 2018, out of which 269 million internet users resides in urban areas while rest 37 million were from rural areas. Mumbai, Delhi and Hyderabad were rated as top cities in internet usage with 12 million, 8.7 million and 7.1 million internet users respectively. About 75% internet users are below the age of 35 years. In India around 81% population is using mobile phones, out of which 10% using smart phone, 9% using multimedia phone and 3% use tablets. About 25 million people accessing internet through mobiles. Indian believes in social networking 86% internet users visit social networking sites.

CONCLUSION

As there is a drastic growth in the e-commerce, internet or cyber security is a major issue in the growing countries like India. According to recent survey , which announced in TOI that India will require five lakh cyber security professionals by 2015 to support its fast growing internet economy as per an estimate by the Union ministry of information technology. The financial sector alone is expected to hire over 2 lakh people while telecoms, utility sectors, power, oil & gas, airlines, government (law & order and e-governance) will hire the rest. Employment news says - Based on academic background and work experience, ethical hackers can don the roles of network security administrators, network defense analysts, web security administrators, application security testers, security analysts, forensic analysts, penetration testers and security auditors. the job role would be to develop and test IT products and services of organizations and ensure that they are as secure as

possible. Secure programming, authorized hacking and network security surveillance are specializations in this domain.

REFERENCES

1. Andrej Savin, EU internet law, Edward Elgar Publishing Limited, Cheltenham, U.K., 2016.
2. Clifford Stoll, The Cuckoo's Egg: Tracking A Spy Through the Maze of Computer Espionage, Knopf Doubleday Publishing Group, Broadway New York, 2012.
3. D. Thomas & B. D. Loader (Eds), Cybercrime: Law Enforcement, Security, and Surveillance in the Information Age, New York: Routledge 2015.
4. David Bainbridge, Encyclopaedia of information technology law, Universal Law Publishing Co. Pvt. Ltd., Delhi, 2018.
5. Faye Fangfei Wang, Internet jurisdiction and choice of law, Cambridge University Press, New York, 2015.
6. Graham J.H. Smith, Internet law and regulation, Sweet & Maxwell, London, 2018.
7. Laurent Garzaniti, (ed.) and Matthew O'Regan, (ed.), Telecommunications, broadcasting and the internet EU competition law and religion, Sweet & Maxwell, London, 2016.
8. Myra Williamson, Terrorism, War and International Law: the Legality of the Use of Force against Afghanistan in 2001, Ashgate Publishing. United Kingdom, 2009.
9. N. Wiener, Cybernetics or Control and Communication in the Animal and the Machine, The Technology Press John Wiley & Sons, Inc., New York, 1948.
10. Peter K. Smith (ed.) & Georges Steffgen, (ed.), Cyberbullying through the new media, Psychology Press, East Sussex, 2018.
11. Peter Lilley, Hacked, Attacked and Abused, Biddles Ltd., Guildford and Kings Lynn, UK 2015.
12. Tim Paul Kevan and Paul Mcgrath, Encyclopaedia of information technology law: e-mail, the internet and law essential knowledge for safer surfing, Universal Law Publishing, New Delhi, 2015.
13. Vakul Sharma, Information Technology: Law and Practice, Universal Law Publication Co., New Delhi, 2012.
14. Verinder Grover, Encyclopaedia of International Terrorism, Deep & Deep Publications, Delhi, Vol. 2, 2014.