IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 5, May 2023

Survey on Need of Cyber Security in India

Pushpdant Sharma
Department of CSE
Dronacharya College of Engineering, Gurugram, Haryana, India

Abstract: In the current world that is run by technology and network connections, it is crucial to know what cyber security is and to be able to use it effectively. Systems, important files, data, and other important virtual things are at risk if there is no security to protect it. Whether it is an IT firm not, every company has to be protected equally. With the development of the fresh technology in cyber security, the attackers similarly do not collapse behind. They are consuming better and enhanced hacking techniques and aim the weak points of many businesses out there. Cyber security is essential because military, government, financial, medical and corporate organizations accumulate, practise, and stock unprecedented quantities of data on PCs and other devices. An important quota of that data can be sensitive information, whether that be financial data, intellectual property, personal information, or other various kinds of data for which illegal access or acquaintance could ensure negative concerns.

Keywords: Cyber security

I. INTRODUCTION

In 2009, compared to physical theft fraudulent money transfers has exceeded in bank branches of United States. Crimes have gone up by 60% every year,in 2012, 3500 cases and 2070 in 2011 reported in India. As per report from National Crime records Bureau (NCRS), Maharashtra reports 561 cases, Andhra 454 cases, Karnataka 437 cases in the year 2012 crimes which are done by age group of 18 to 30[18].Haryana registered 3 cases in 2011 but 116 in the year 2012 which is a drastic raise. Compared to other crimes, this cyber crime doesn't require much investment and can be done in various locations. These crimes originate from various sources and exhibits socio-educational/economic and technological factors including addiction which also includes counterfering, economic crimes, money laundering, child pornography, sexual exploitation, drug trafficking, human trafficking, terrorism, fraud etc.

1.1 Why Cyber Crime is more now days?

There are 5 common trends which give chances to cyber crime:

More online transactions and digital data. Transaction and customer information, results of product launches, and other market information are easily available. Creating valuable intellectual property online is an attractive target.

Comparatively Corporations and companies are expected to be more transparent than before. Majority of people want to access to corporate networks through their mobile devices for day to dayactivities.Though smarter technology devices increases connectivity and but present latest types of security threats. Hackers can crack these securities and get an easy entry into corporate networks.

Malicious Software like viruses and spyware are strong enough to take the partial control of main applications.

In business, customer and vendors are joined to the networks to increase their business profits. In December 2010, a famous E-business website was attacked by dozens of people claiming to be part of the unnamed group. They attempted to perpetrate a denial of service attack in retaliation for website to shut down payment services to other websites. More than a dozen hackers were arrested in that crime.

There is more technology advanced hackers, professional cyber crime organization. For example, hacker receives payment to infect end user device with malware. Today's Malwares are difficult to trace and they steal data for financial gain. Some people think that they get more money if they become hackers compared to securers.

DOI: 10.48175/IJARSCT-10050

II. 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 authenticatinginformation 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.

III. 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

DOI: 10.48175/IJARSCT-10050

air forces is well defined. Outer space and cyberspace are different. They are inherently international even from the perspective of national interest.

IV. METHODS OF ATTACKS AND AVOIDANCE

The most popular weapon in cyber terrorism is the use of computer viruses and worms. That is why in some cases of cyber terrorism is also called 'computer terrorism'[1]. The attacks or methods on the computer infrastructure can be classified into three different categories.

(a) Physical Attack. The computer infrastructure is damaged by using conventional methods like bombs, fire etc.

(b) Syntactic Attack. The computer infrastructure is damaged by modifying the logic of the system in order to introduce delay or make the system unpredictable. Computer viruses and Trojans are used in this type of attack.

(c) Semantic Attack. This is more treacherous as it exploits the confidence of the user in the system. During the attack the information keyed in the system during entering and exiting the system is modified without the user's knowledge in order to induce errors.

The first step in protecting yourself is to recognize the risks and become familiar with some of the terminology associated with them.

- **Viruses** - This type of malicious code requires you to actually do something before it infects your computer. This action could be opening an email attachment or going to a particular web page.
- **Worms** - Worms propagate without user intervention. They typically start by exploiting a software vulnerability (a flaw that allows the software's intended security policy to be violated), then once the victim computer has been infected the worm will attempt to find and infect other computers. Similar to viruses, worms can propagate via email, web sites, or network-based software. The automated self-propagation of worms distinguishes them from viruses.
- **Trojan horses** - A Trojan horse program is software that claims to be one thing while in fact doing something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder.
- **Hacker, attacker, or intruder** - people who exploit weaknesses in software and computer systems for their own gain. Though they do it for curiosity,their actions are typically in violation of the intended use of the systems. The results can range from creating a virus with no intentionally negative impact to stealing or altering information.
- **Malicious code** - This category includes code such as viruses, worms, and Trojan horses. Although some people use these terms interchangeably, they have unique characteristics.

E-Mail Related Crime- Certain emails are used as host by viruses and worms. E-mails are also used for spreading disinformation, threats and defamatory stuff.

Denial of Service -These attacks are aimed at denying authorized persons access to a computer or computer network.

Cryptology-Terrorists have started using encryption, high frequency encrypted voice/data links etc. It would be a Herculean task to decrypt the information terrorist is sending by using a 512 bit symmetric encryption.

V. 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 2011 Census, Only 3.1 percent of total houses have Internet access in India. The census covered 24,66,92,667(246.7 million) houses in India and found only 76,47,473 (3.1%) of this houses use Internet. The Internet includes both broadband and low-speed connections.

According to Internet World Stats on June 30 2012, there were 2.4 billion internet users (2,405,510,175) worldwide. China was the largest countries in terms of internet users with over 538 million users[19]. The following graph (figure 1) shows top 20 internet countries worldwide at mid-year 2012:

DOI: 10.48175/IJARSCT-10050

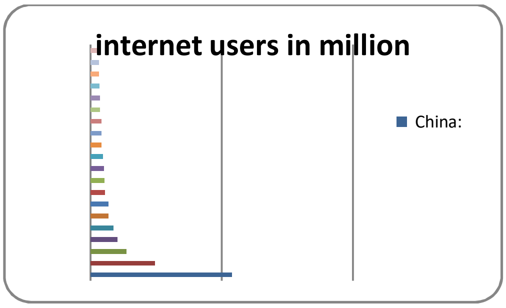


Figure 1: Internet usage in top countries world-wide at year 2012.

Following graph (figure 2) shows the growth of E-commerce in India, in 2011 it has reached 10000 million USD.

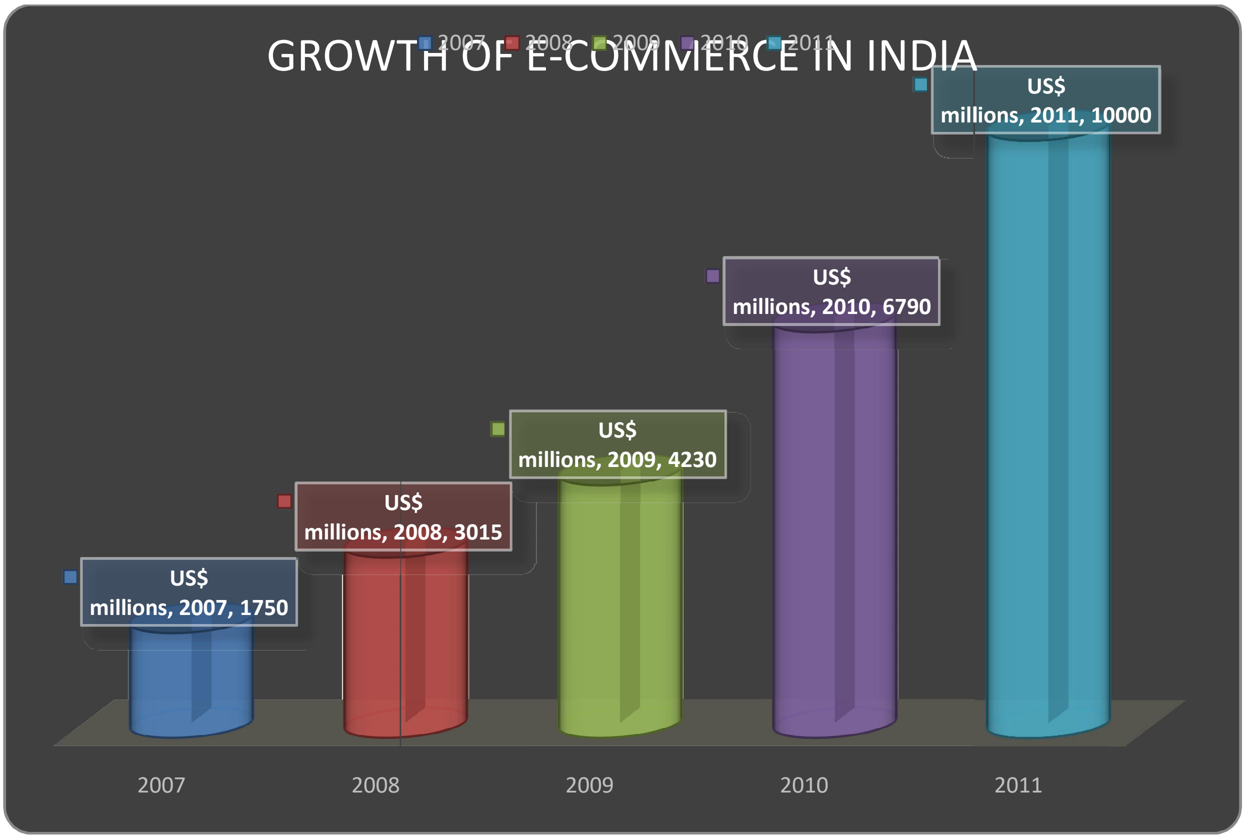
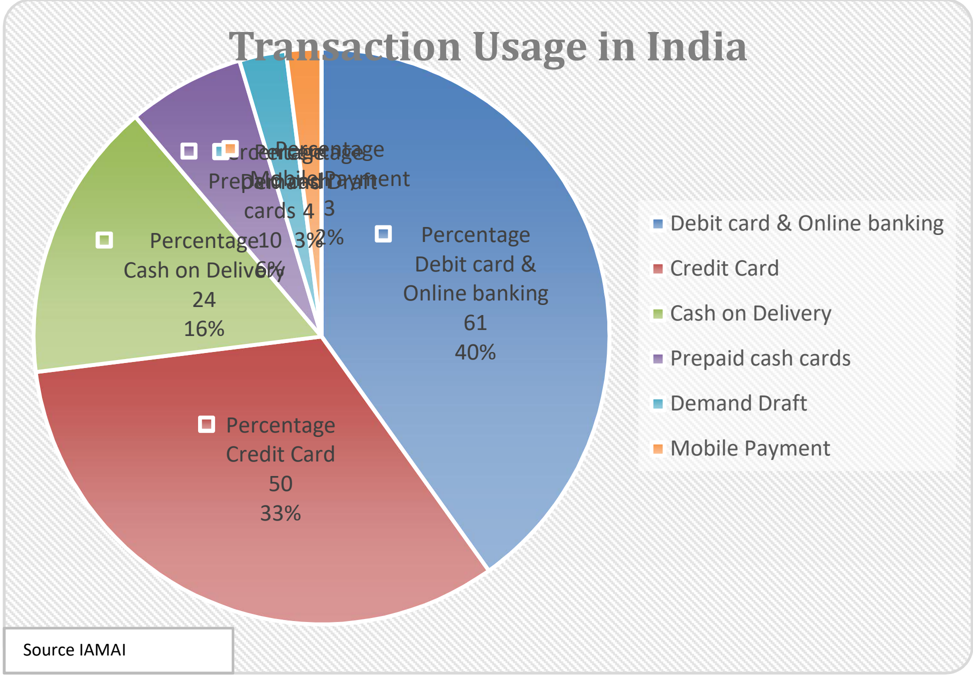


Figure 2: Increasing usage of E-commerce in India

Most of today's transactions are online. The following graph (figure 3) shows Indian payment type in the year 2012 according to which is online transactions is more[8].



Source IAMAI

Figure 3: Percentage of usage of different online payment methods in India

With all these statistics ensures that India as a fast growing country especially in the field of information technologies and E-commerce has a high alert for Security for its online channels to monitor over frauds and financial losses.

VI. CYBER SECURITY INITIATIVES IN INDIA

ISO 27001 (ISO27001) is the international Cyber security Standard that provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System.

6.1 India's legal framework for cyber security.

Indian IT Act, 2000

Section 65 - Tampering with computer source code, Section 66 - Hacking & computer offences, Section 43 – Tampering of electronic records

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.

Indian Penal Code

Section 406 - Punishment for criminal breach of trust and Section 420 - Cheating and dishonestly inducing delivery of property[6].

Indian Contract Act, 1872

Offers following remedies in case of breach of contract, Damages and Specific performance of the contract

6.2 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[6]. 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[5]. This Platform and Website is managed by

Perry4Law, Perry4Law Techno Legal Base (PTLB) and Perry4Law Techno Legal ICT Training Centre (PTLITC)[12]. 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[7]. 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[11]. 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.

6.3 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[15].

6.4 Top colleges which offer cyber security course in india[17]

- Indian Institute of Information Technology - Allahabad, Uttar Pradesh
  Master of Science in Cyber Law and Information Security
- The Indian Institute of Information Technology Allahabad - Allahabad, Uttar Pradesh
  Master of Science in Cyber Law and Information Security
- Institute of Management and Technology - Ghaziabad, Uttar Pradesh
  MS in Cyber Law and Security
  Post Graduate Diploma in Cyber Security
- Amrita School of Engineering - Coimbatore, Tamil Nadu
  Master of Technology- Cyber Security
- Amity University - Noida, Uttar Pradesh
  M.Tech - Information Security & Cyber Forensics
- Faridabad Institute Of Management Studies - Faridabad, Haryana
  Post Graduate Diploma in Cyber Security
- Institute of Management Technology - Ghaziabad, Uttar Pradesh
  Post-Graduate Diploma in Cyber Security
- Sarvodaya Law College - Bangalore, Karnataka
  Post Graduate Diploma in Cyber Law and Information Technology

DOI: 10.48175/IJARSCT-10050

VII. 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.