Cyber Education: A Need of the Time

Parveen Sadotra, Chandrakant Sharma

Abstract: -In the last two decades Internet has changed our lives in a great way. Almost everything is dependent on internet. Vast use of internet has created a new kind of threat to human civilization. Dependency of our day to day work in cyber world has become indispensable in present time. This revolution of internet has made our life much easy on one hand but at the other hand we need to be very much cautious. If we are not familiar of the pros and cons of the cyber world it may cost a huge loss sometimes to even life. So it is the need of time that every one of this earth should educated well about this beautiful cyber world along with all the security aspects and it needs a well-planned strategy to achieve 100 % cyber literacy.

Keywords: - Cyber Education, Cyber Security, Cyber Theft, Cyber World, Literacy.

I. INTRODUCTION

Everyone knows invention of Internet is one of the biggest things for human evolution on this planet. It is the latest technology for communication which has made our lives easier. In present times we are dependent on almost everything in each field viz. education, health, defense, aviation banking, travel, social interaction, media and so on list is endless. Where ever we go internet follows. Earlier we were talking about literacy but now we talk about cyber literacy, because now days not a single person is untouched from cyber world. He/she is at any place on this earth but somehow in touch with cyber world. Cyber invention has made our life so dependent on it that we cannot think of our life without it. Cyber world has given us so many things in very simplified manner but same time there has been a new negative development in it. Lots of information is kept online now days which has invited to a kind of new threat to us. Theft of private information, theft of money from banks and other invasion on private life has made us to think for a planned and proper education of cyber world to all of us.

II. NEED / IMPORTANCE OF THE STUDY

Internet is one of the fastest-growing areas of technical infrastructure development. In today's business environment, disruptive technologies such as cloud computing, social computing, and next-generation mobile computing are fundamentally changing how organizations utilize information technology for sharing information and conducting commerce online. Today more than 80% of total commercial transactions are done online, so this field required a high quality of security for transparent and best transactions. The scope of Cyber Security extends not only to the security of IT systems within the enterprise, but also to the broader digital networks upon which they rely including cyber space itself and critical infrastructures.

Cyber security plays an important role in the development of information technology, as well as internet services. Enhancing cyber security and protecting critical information infrastructures are essential to each nation's security and economic well-being. Society has become dependent on cyber systems across the full range of human activities, including commerce, finance, health care, energy, entertainment, communications, and national defense . Recent research findings also show that the level of public concern for privacy and personal information has increased since 2001 Internet users are worried that they give away too much personal information and want to be forgotten when there is no legitimate grounds for retaining their personal information.

Following are the main reasons as why we feel there is need to the study importance cyber security education: -

- Increased usage of internet more than 80 % of the things are done today through internet
- Increased dependency on the use of internet
- Almost all the commercial additives are done online in present time
- Increased use of social networking websites where lots of personal information is posted by individuals without knowing the theft and misuse of this information
- A phenomenal increase in the cybercrime all over the world
- Security can't be guaranteed it has to be practiced by imparting education to all the people directly or indirectly involved with internet
- Safety of personal information
- With all the news stories about hackers, botnets, and breaches involving personal information, it's easy for the security message to sound over-used and tired. It's easy for people to say, "It won't happen here." Yet, studies and surveys repeatedly show that the human factor (what employees do or don't do) is the biggest threat to information systems and assets.
- Protecting unauthorized access, disclosure, modification of the resources of the system.
- Security during on-line transactions regarding shopping, banking, railway reservations and share markets.
- Security of accounts while using social-networking sites against hijacking.
- The changing shape of cyber security education: Colleges, government attempt to address industry shortage.
- The Global Information Security Workforce has predicted that over the next three years, demand for personnel with relevant security skills may rise 13 percent each year.

Revised Version Manuscript Received on February 22, 2016.

Parveen Sadotra, Certified Ethical Hacker, Jammu (J&K), India.
Dr. Chandrakant Sharma, Assistant Professor, Career Point University, Kota (Rajasthan), India.

- Overall, the market for cyber security professionals may be growing 12 times faster than the U.S. job market as a whole.

Both the public and private sectors are fervently seeking cyber educated employees in various forms as operators, programmers, security expertise, but instilling it in college students and employees seeking additional training can take time. The gold standard Certified Information Systems Security Professional, for instance, requires four years of experience to obtain and many firms cannot afford to wait that long to fill the gaps in their ranks their requirements.

III. STATEMENT OF THE PROBLEM

How should people be educated about cyber security? It is a problem in India. India still lacking 100 % literacy, in such case educating about cyber threat and its security is a big problem. Following are the main problems faced fur imparting education about cyber security: -

- Lack of sufficient trained manpower to educate other people
- Availability of cyber institutes. Though urban areas have advanced significantly but rural areas still lack good institutions.
- Lack of infrastructure. India still relies on a tortoise speed on internet. 3G speed of on internet is also not good as it was said, whereas 4G is in its launch phase.
- Lack of concrete government policy for cyber education
- Lack of sufficient hardware in government educational institutes
- Motivation is another factor in older employees of government and private sector to keep pace with new technology. They don't want to learn new things.
- Lack of cyber curriculum in government educational institutes
- Cyber security skills in demand as threat environment become more complex, while cyber security experts seem to be in short supply at the moment, malware and cyber-attacks do not.
- Every day a new challenges for Cyber security professionals
- People still opt other fields for their career like engineering and Medical or management instead of choosing cyber world as theirs.
- There is a big gap in Demand and supply of cyber security trained people in India
- Medium if teaching is also another problem for Indian society. There are still a large number of people who can communicate in Hindi or in their own language whereas Cyber education needs English language.
- Both the public and private sectors are fervently seeking cyber security expertise, but instilling it in college students and employees seeking additional training can take time. The gold standard Certified Information Systems Security Professional, for instance, requires four years of experience to obtain, and many firms cannot afford to wait that long to fill the gaps in their ranks.
- There are some ethical and legal issues too.
- The advancement in technologies supported the intruders or hijackers in the better understanding of the current cyber security methods

IV. OBJECTIVES

Cyber Education means imparting specialized knowledge to all the people who can well understand using computers and internet and at the same time understanding the threat perception involved in it and keeps themselves safe in this ever growing interconnected world of cyber systems. As we know, there is a lot of work to be done in field of cyber education in India. The main objective of this paper is to find out present state of cyber education in India, what are problems faced for carrying out cyber education and search for appropriate course of action in this field.

V. HYPOTHESIS

Most IT security management approaches consist of checklists which decision makers use to develop a coverage strategy; these generally are little more than a triage approach to categorizing threats. One popular hypothesis for risk visualization has been the construction of a risk cube, where each axis or dimension represents one of the three components of risk (threats, assets, and vulnerabilities) and the volume of the cube represents the amount of risk These Models have been developed which attempt to deal with risk analysis in a qualitative manner. Mark Egan (Ex CTO for Symantec) in his book The Executive Guide To Information Security introduced a very simple tabular model which allows users to rate threat severities into one of three categories/columns (low, medium and high) and then to average across columns. This simple triage approach to subjective threat impact analysis, though insightful, is notable to capture system uncertainty which helps us to design our cyber education system. Alberts and Dorofee developed system called OCTAVE which also utilizes qualitative information to assess risk. Others have tried approaches that quantify IT security risk analysis. Beauregard applied the Value Focused Thinking (VFT) approach from general risk analysis to assess the level of information assurance within the Department of Defense units.

VI. RESEARCH METHODOLOGY

In this paper a case study approach was used insights into the phenomenon, in this case present and future state of cyber education. Quality inquiry methods were used in our study. These methods enabled us to capture an understanding of the perspective regarding cyber education in India. Some Interviews were also conducted to conclude about present status of the cyber education with general public and experts. We also utilized internet to get some insight on the topic. We also visited some cyber education institutes in rural and urban areas and contacted some government and private schools to identify the issues in this field in our country. Total 100 people were interviewed, 10 schools were contacted and 12 cyber institutes visited.

This paper has examined the significance of privacy for individuals as a fundamental human right. Violations of human rights arise from the unlawful collection and storage of personal data, the problems associated with inaccurate personal data, or the abuse, or unauthorized disclosure of such data. In this paper we also include the current threats, issues, challenges and measures of IT sector in our society. With the increasing incidents of cyber-attacks, building an effective intrusion detection model with good accuracy and real-time performance are essential

VII.RESULTS AND DISCUSSION

Sl. No.	Description	Percentage	
		Urban Sector	Rural Sector
1	IT literate people	50 %	5 %
2	IT literate below 20 Yrs. of age	90 %	30 %
3	Aware of cyber security	12.4 %	0.75 %
4	Cyber education institute	1 per 10000 population	1 per 2.6 Lacs population
5	Infrastructure of cyber education	More organized and available	Not in proper way
6	Use of social networking websites	Approx. 65 %	Approx. 8 %
7	Use of Net Banking	Approx. 8 %	Approx. 0.2 %
8	Online shopping	5 %	Zero
9	Availability of cyber education in primary schools	80 %	Zero
10	Use of email	75 %	9.5 %

Data in above table shows the condition of cyber education in our country. We are far behind from developed countries in terms of usage of Information technology and cyber education. We have to work hard to bring our country to a minimum required level. We can see there are very few people in rural areas that use internet and emails. Use of Social networking websites is also very less.

VIII. FINDINGS

Following are the findings of the research: -

- There are more cyber educated people in urban sector than rural sector
- Rural sector has lesser training facilities
- More advance courses are available in urban institute only
- Young people are more educated about information technology
- Use of net has increased substantially in urban area but people in rural areas still away from it (very few people use internet)
- There is no concrete policy direction by government on cyber education.
- Awareness about cyber security aspect is almost negligible in India.
- Use of smart phones has made it possible for increment in internet
- Instance of cyber theft and hacking has increased very in recent years
- Many people among us have faced any kind of hacking or information theft from their account.
- Government schools lack sufficient infrastructure of cyber education. These school also lack well trained cyber teachers.
- Many people in rural areas don't know about computer virus, malware, theft of information and about hacking.
- Mark Zukerberg may be boasting that he has brought world together with the help of Facebook but condition in India is not so good especially in sub-urban and rural areas of country.

IX. RECOMMENDATIONS/ SUGGESTIONS

Based on the survey made and our findings about present state of use of cyber technology and cyber education in India, we can see a lot need to be done in this field. It is time to need proper cyber education in our country. Following recommendations are made to improve cyber education system in India: -

- Government need to formulate a concrete policy and guidelines for the imparting cyber education in India starting from primary school.
- We security need to focus on sub urban and rural areas for opening more cyber education institutes.
- Advance courses should be started in rural areas
- People need to be made aware of this cyber world, its usefulness along with security aspects.
- Government employee especially elderly people need to be motivated to learn latest technology to enhance productivity.
- High speed internet should be made available at cheaper rates by mobile companies.
- IT Act 2010 needs to be reviewed again as cybercrimes are on rise day by day. We need to make more strict rules.
- In institutes, schools and colleges emphasis should be given on cyber security too as cybercrimes are growing day by day in our country.
- There should be more Conferences and symposiums on cybercrime and cyber security to make people aware of latest developments
- People needs to make aware for sharing information on various platforms of internet like social networking sites, emails etc

X. CONCLUSIONS

India is a developing country but the use of information technology is increasing at very fast pace. Increased use of IT has made us more dependent on it in all the fields.

There is also increase in hacking activity so cyber security aspect should not be ignored. Indian citizens must identify the best methods for cyber education and effective techniques in order to protect the information and systems, as well as the network in which they work. The IT industry has been playing catch-up with hackers and cybercriminals for decades. Thus there is a need of cyber security curriculum in the near future which will in-build the cyber-security understanding in the current youth and finally the IT sector will get more profound, securely skilled professionals not only in the security sector but also in the every sector, thus enhancing the communication, the brain compatibility skills of the employees and the employers. Effective cyber-security policies, best practices for cyber education must be planned and most-important must be implemented at all levels. In the future the Government role and education systems participation in the cyber education and security awareness approach will lead to an IT literate and strongly secured nation.

SCOPE FOR FURTHER RESEARCH

There is always scope for improvements in every sector at each level. Cyber world is a vast field in present time and there is lots of research work needs to be done. We have lots of scope to make research on Cyber theft, cybercrime, cyber security, forensic research, retrieval of data, website development, programming languages, scope for online business, online education and so on, List is huge in the present time. But first requirement is to enhance quantity and quality of cyber education in India. Lots of people are opting cyber world as their career but there is still more scope of career in various fields in IT sector.

REFERENCES

1. <http://ijcse.academic-publication.org/>
2. <http://www.nativeintelligence.com/ni-programs/whyaware.asp>
3. Parveen Sadotra (CEH), Prof. Vinus Sharma, 2015, *"Measuring And Combating Spam on Social Networks"*, 'Cyber Times International Journal of Technology & Management', Vol 8. Issue 1. Pg.28-32
4. <http://deity.gov.in/content/information-security-education-and-awareness-project
5. <https://tdloffice.wordpress.com/2013/10/21/trust-in-digital-life-introduction/>
6. Parveen Sadotra (CEH), Dr. Anup Girdhar, 2015, *"Role Of Cyber security In Private sector Domains"*, 'Cyber Times International Journal of Technology & Management', Vol 8. Issue 1. Pg.7-11.
7. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.159.6388&rep=rep1&type=pdf>
8. <http://www.witdom.eu/tdw2015>
9. <http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?reload=true&punumber=6883276>
10. <http://www.pewinternet.org/2014/03/11/digital-life-in-2025/>
11. Parveen Sadotra, 2015. Research Challenges and Issues in Web Security. International Journal of Computer Engineering & Technology (IJCET).Volume:6, Issue: 5, Pages: 1-7