Volume 5, Issue 12, December 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Ascertaining Awareness of Cybersecurity and Cyber Threats in Uttarakhand

Dr. Jeetendra Pande*
School of CS & IT, Uttarakhand Open University,
Haldwani, Uttarakhand, India

Abstract— With the growth of internet, the dependence on computers has increased exponentially. The advancement of technology is being equally enjoyed by cyber criminals leading to new forms of threats. The challenge is to protect critical information infrastructure, like civil aviation sector, Railways' passenger reservation system and communication network, port management, companies and organisations in power, oil and natural gas sectors, banking and finance, telecom sector, etc. from cyber attacks. This paper attempts to investigate the current status of cyber crime at International level, National level and in Uttarakhand. The paper recommends the imperativeness of creating mass awareness about cyber security and evaluates the possibility of using Massive Open Online Course (MOOCs) as an effective measure for spreading mass awareness about cyber security.

Keywords— Cyber Security, MOOC, Cyber attack, Malware, Uttarakhand.

I. INTRODUCTION

With the advent of Internet, the rules of business have changed. Due to the reach and coverage of Internet, more and more processes in large, multi-national organizations are going online. With increased dependence on computers and Internet, these organizations are constantly exposed to high levels of business, operational and strategic risks. Cyber space is virtual, borderless and anonymous, due to which it becomes difficult to trace the specific origin of a cyber attack. Thus, it is a challenge for these organizations to protect their data and systems from unauthorized access.

Large national and international organizations, which have large budget allocation of IT & Information Security, like AT&T, Google, Apple, Domino's Pizza, JP Morgan Chase, Sony, etc. have fallen prey to organised cyber crime.

Computer Emergency Response Team-India (CERT-In) has reported that during the year 2015, as many as 54,483 cyber security incidents such as phishing, spam and malicious code have been reported**[19]**. The number was 22,060 in 2012, 71,780 in 2013, 1,30,338 in 2014, respectively. It further reports that large number of Indian websites have been hacked in the recent years, i.e., 21,699 in 2011, 27,605 in 2012, 28481 in 2013, 32,323 in 2014 and 9,057 in 2015(up to May)[3]. These attacks have been observed to be originating from the cyber space of a number of countries, including the US, Europe, Brazil, Turkey, China, Pakistan, Bangladesh, Algeria, Saudi Arabia, Morocco and the UAE. The ease of online banking and transactions has brought with it a significant rise in malicious attacks on digital devices and software systems. Most of these attacks, as recent instances of online thefts have demonstrated, have been in the banking and financial services domain. Arbor Networks' research report states that 2013 witnessed a huge rise in attacks against the banking and financial services sector. Government establishments also faced such attacks. The firm said there was a 136% increase in cyberthreats and attacks against government organizations and 126% against financial services organizations in India. Experts have recognized that malicious file inclusions, malware distribution and distributed denial of services (DDOS) attacks are known threats that can arise out of improper file handling and such threats are often used to synchronize attacks on websites or large networks, the report stated [2].

II. REVIEW OF THE CURRENT STATUS

A. International Status

A survey by Kaspersky Lab and B2B International finds that 91 percent of organizations polled suffered a cyber-attack at least once in the preceding 12-month period[9]. In May 2000 the IC3 initiated operations as a centre to receive complaints of Internet crime. The IC3 received its one millionth complaint seven years later, in June 2007, and its two millionth complaint in November 2010. Over the last five years the IC3 received an average of nearly 300,000 complaints per year. The complaints consist of a wide array of Internet scams touching victims of all nationalities, ages, backgrounds, educational levels, and socio-economic levels. In 2013 alone, the verifiable dollar loss of complaints submitted to the IC3 totalled nearly $800 million. The total dollar loss claimed from all complaints over the life of the IC3 exceeds $2 billion[7].

KMPG report reviled that Cyber war and espionage against governments is on the rise throughout the globe. It reported that the US defence system has been targeted on several occasions. Similarly, Canada has also been a victim of a cyber attack[12]. According to the Crime Survey for England and Wales (CSEW), the proportion of adult internet users reporting a negative online experience declined from 39 per cent in 2010/11 to 37 per cent in 2011/12 [14].

B. National Status

With the growth of internet, the dependence on computers has increased exponentially. The challenge is to protect critical information infrastructure, like civil aviation sector, Railways' passenger reservation system and communication network, port management, companies and organisations in power, oil and natural gas sectors, banking and finance, telecom sector, etc. from cyber attacks.

India is ranked fourth among the top 50 countries in terms of the number of cyber crime complaints reported to the Internet Crime Complaint Centre (IC3), preceded only by the US, Canada and the UK based on the 2014 IC3 annual report [23].

Shortage of trained cyber security workforce is of serious concern to India. In comparison to China, US and Russia that have 125000, 91080 and 7300 trained cyber experts respectively; India has merely 556 cyber experts deployed in various government agencies[25]. India is considered an IT superpower that is a major exporter of software and hosts major ITES-based outsourced businesses. Therefore, IT constitutes a major share of Indian economy. Recently, European Union has picked holes in India's data security system and suggested that a joint expert group be set up to propose ways on how the country should tighten measures for qualifying as a data secure nation[26]. Therefore, India needs look seriously into upgrading its Information Security infrastructure and reframe cyber policies to get data secure status from EU. This is crucial for India to retain high-end outsourced business, which has a potential of increasing from the existing $20 billion to $50 billion.

Another dimension of 'Information and Cyber Insecurity' is net-banking frauds or e-frauds. According to the Delhi Police, as many as 200 complaints of netbanking frauds are received every year, but a few are actually registered. According to recent media reports, unauthorized transactions totalling nearly INR 30 crore (USD 0.3 billion) have been conducted on credit cards of Indian customers and a global syndicate is said to have been behind these frauds. Since 2009, cyber criminals have defrauded banks in the country of almost INR 130 crore. The Ministry of Finance, Government of India has registered a record 32, 928 cases of frauds pertaining to ATMs, debit and credit cards as well as net-banking involving 50 nationalized and other banks across country [22].

The table below displays the data received from National Crime Records Bureau, which verifies the increasing trend of cyber crime.

TABLE I INCIDENCE OF CASES REGISTERED UNDER CYBER CRIMES IN STATES/UTS DURING 2012 & 2013 AND PERCENTAGE VARIATION[15]

Sl.No.	State/UT	IT ACT		
		2012	2013	% Variation
(1)	(2)	(3)	(4)	(5)
STATES:				
1	ANDHRA PRADESH	429	635	48.0
2	ARUNACHAL PRADESH	12	10	-16.7
3	ASSAM	28	154	450.0
4	BIHAR	23	23	0.0
5	CHHATTISGARH	49	91	85.7
6	GOA	30	57	90.0
7	GUJARAT	68	61	-10.3
8	HARYANA	66	112	69.7
9	HIMACHAL PRADESH	20	24	20.0
10	JAMMU & KASHMIR	35	46	31.4
11	JHARKHAND	10	13	30.0
12	KARNATAKA	412	513	24.5
13	KERALA	269	349	29.7
14	MADHYA PRADESH	142	282	98.6
15	MAHARASHTRA	471	681	44.6
16	MANIPUR	0	1	@
17	MEGHALAYA	6	17	183.3
18	MIZORAM	0	0	@
19	NAGALAND	0	0	@
20	ODISHA	14	65	364.3
21	PUNJAB	72	146	102.8
22	RAJASTHAN	147	239	62.6
23	SIKKIM	0	0	@
24	TAMIL NADU	39	54	38.5
25	TRIPURA	14	14	0.0
26	UTTAR PRADESH	205	372	81.5
27	UTTARAKHAND	4	23	475.0
28	WEST BENGAL	196	210	7.1
	TOTAL (STATES)	2761	4192	51.8

UNION TERRITORIES :				
29	A & N ISLANDS	2	18	800.0
30	CHANDIGARH	33	9	-72.7
31	D & N HAVELI	0	0	@
32	DAMAN & DIU	0	1	@
33	DELHI	76	131	72.4
34	LAKSHADWEEP	0	0	@
35	PUDUCHERRY	4	5	25.0
	TOTAL (UTS)	115	164	42.6
	TOTAL (ALL INDIA)	2876	4356	51.5

C. Uttarakhand Status

A security survey for Uttarakhand was conducted through online questionnaire between September 2014 and June 2015. The survey covered 595 respondents from 13 districts covering school & college students, government employees, housewives, teachers, businessmen and professionals. The district wise participation was as follows:

TABLE II THE DISTRICT WISE PARTICIPATION

S.No.	District	No. of Participants	%
1	Almora	43	7.23
2	Bageshwar	18	3.03
3	Chamoli	17	2.86
4	Champawat	20	3.36
5	Dehradun	75	12.61
6	Haridwar	50	8.40
7	Nainital	194	32.61
8	Pauri Gharwal	21	3.53
9	Pithoragarh	30	5.04
10	Rudraprayag	14	2.35
11	Tehari Gharwal	18	3.03
12	Udham Singh Nagar	60	10.08
13	Uttarkashi	35	5.88
Total		595	100

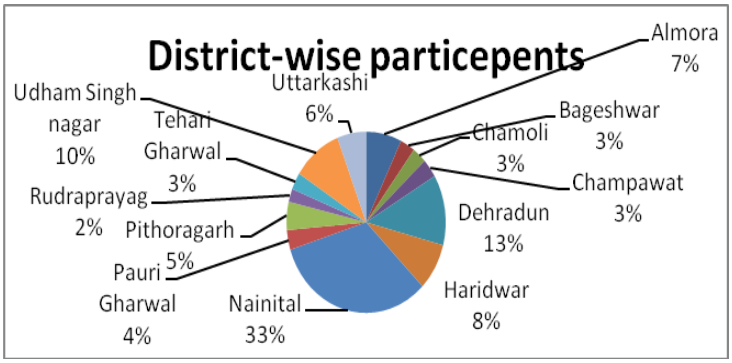

Fig 1 District wise participation

The gender wise profile of the participants was as follows:

TABLE III DETAILS OF GENDERWISE PROFILE OF THE PARTICEPENTS

S. No.	Gender	No. of participants	%
1	Male	391	65.71
2	Female	205	34.29
Total		595	100

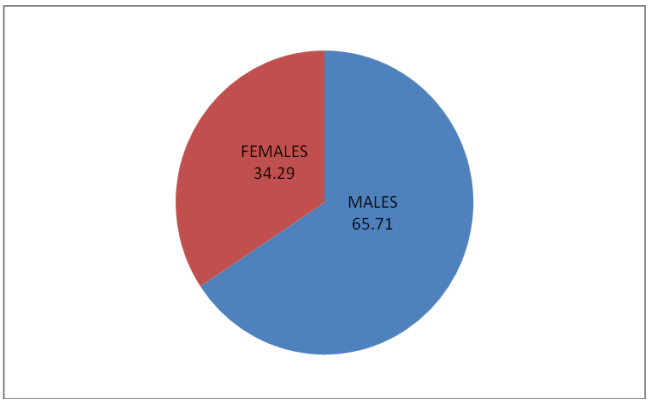

Fig 2 Graphical representation of gender-wise profile of the participants

The details of profile of the participants, based on their age group, are as follows:

TABLE IV AGEWISE PROFILE OF THE PARTICEPENTS

S. No.	Age Group(in years)	No. of participants	%
1	05-24	257	43.19
2	25-34	244	41.00
3	35-44	81	13.61
4	45-54	06	1.01
5	55-64	04	0.67
6	65-74	01	0.16
7	75 and above	02	0.33
Total		595	100

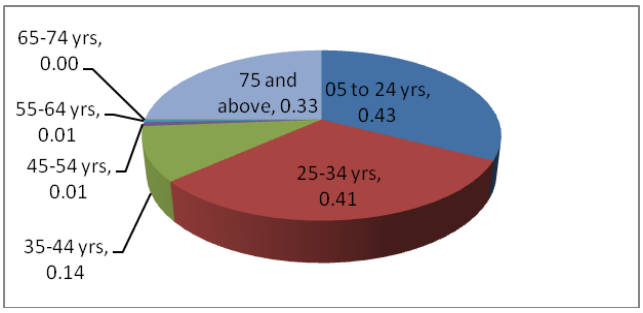

Fig 3 Graphical representation of Agewise profile of the particepents

TABLE V EDUCATIONAL PROFILE OF THE PARTICEPENTS OF THE SURVEY

S. No.	Education Qualification	No. of respondents	%
1	Below 10^{th}	1	1.84
2	12^{th} pass	101	16.97
3	Graduate	206	34.62
4	Post Graduate	243	40.84
5	PhD	44	7.39
Total		595	100

Responses of the participants to the survey question are as follows:

TABLE VI DETAILS OF THE RESPONSE OF THE SURVEY PARTICIPENTS

S. No.	Incident/Event	Number of positive responses	%
1	Have you ever been a victim of any of cyber Stalking?	199	33.44
2	Have you ever been a victim of cyber terrorism?	22	3.69
3	Have you ever been a victim of Forgery and Counterfeiting?	101	16.97
4	Have you ever been victim of piracy and IPR related crimes?	60	1.01

5	Have you ever been a victim of Phishing, Vishing or Smishing?	172	28.90
6	Have you ever been a victim of Computer Vandalism(गुंडागिरी)?	50	8.40
7	Have you ever been a victim of hacking?	205	34.45
8	Have you ever been a victim of spamming?	379	63.69
9	Have you ever been a victim of cross site scripting?	102	17.14
10	Have you ever been a victim of online auction fraud?	187	31.42
11	Have you ever been a victim of Web Jacking?	67	11.26
12	Have you ever been a victim of internet time thefts?	48	8.06
13	Have you ever been victim of denial of service attack?	97	16.30
14	Have you ever victim of data diddling?	68	11.42
15	Have you ever been a victim of salami attack?	17	2.85
16	Have you ever been a victim of email spoofing?	109	18.31
17	In case, you are victim of any of the above, have you ever reported the crime?	59	9.91
18	Do you know how and where to report a cyber crime?	157	26.38
19	Are you interested in a free course on cyber and information security awareness?	540	90.75
20	In what mode you would prefer the course on cyber and information security awareness?	Either Online or Both Online and Offline : 498	83.69

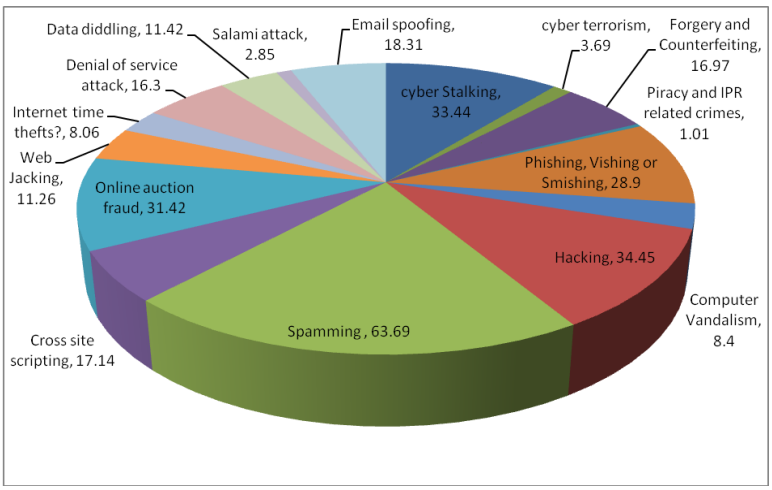

Fig 3 Graphical representation of the %wise response of the particepents

1) Result and Analysis of the Survey

The major highlights of the survey are:

- About 66% of respondents reported that they have been victims of spamming.
- More than 34% of the respondents were victims of hacking.
- Approximately 18% of the participants said they were victims of email spoofing.
- More than one-third of the respondents have experienced cyber stalking.
- Less than 12% have targeted for web jacking.
- The study tells us that not many people, less than 3%, have been victims of salami attacks.

- From the study, we can see that less than 10% of the victims have reported the cyber crime to the competition authority. The major reason for this is lack of awareness, as only 26% reported knowing how and where to report a cyber crime.
- Almost one-third of the participants were victims of online auction fraud.
- More that 80% of the respondents belong to the age group 5-34 years (considered to be most active on internet) and amongst them 32.53% have been victims of cyber stacking and 34.53% have been victims of hacking.

III. IMPORTANCE OF CYBER SECURITY AWARENESS INITIATIVES

The advancement of technology is being equally enjoyed by cyber criminals leading to new forms of threats. *Norton Cyber Crime* Report reveals that in 2012, approximately 42 million people became victims of cyber-attacks in India, having a direct financial implication of USD 8 billion[22].

With continuous increase in the use of IT for business, the dependence of large organizations on complex Information System infrastructure has been growing steadily. These organizations need to update their workforce and infrastructure at a rapid paced, patching up with new network and system vulnerabilities. This is essential in order to protect their sensitive data and hence the business from being compromised by hackers.

India has seen significant increase in attacks against financial and government organizations , with 34% and 43% of them reporting cyberthreats and attacks respectively, up from last year's 15% and 19%, the report revealed [2]. India comes second on the list of countries most prone to cyber attacks on mobile devices organizations , with a major chunk of these intrusions designed for phishing and stealing banking details, a report by security software maker Kaspersky said. Russian cyber security solutions firm Kaspersky Lab said Russia topped the list of attacks on mobile phones, accounting for 40.34 per cent of all attacked unique users. India, with 7.9 per cent of attacks, stood at the second spot, followed by Vietnam (3.96 per cent), Ukraine (3.84 per cent) and the UK (3.42 per cent). Other countries in the top 10 included Germany (3.2 per cent), Kazakhstan (2.88 per cent), the US (2.13 per cent), Malaysia (2.12 per cent) and Iran (2.01 per cent). During 2013, nearly 100,000 new malicious programs for mobile devices were detected, more than double the previous year's figure of 40,059 samples, Kaspersky said [20]. Cyber attacks originating from India rose by 26 per cent in the first quarter of this year, according to a report by cloud services company Akamai, which ranked the country seventh in the top ten list[16]. According to figures compiled by the National Crime Records Bureau (NCRB), cases of hacking registered an increase of 1850% - from just two cases in the year 2010 to 39 in 2011[15].

IV. CONCLUSION, DISCUSSION AND RECOMMENDATIONS

Over the years, Information Technology has transformed the global economy and connected people and markets in ways never imagined earlier. With Information Technology gaining the centre stage, nations across the world are experimenting with innovative ideas for economic development and inclusive growth. It has also created new vulnerabilities and opportunities for its disruption. Cyber security threats emanate from a wide variety of sources and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and governments alike. Their effects carry significant risks for public safety, security of nation and the stability of the globally linked economy as a whole. The origin of a disruption, the identity of the perpetrator or the motivation for it can be difficult to ascertain as the act can take place from virtually anywhere. These attributes facilitate the use of Information Technology for disruptive activities. As such, cyber security threats pose one of the most serious economic and national security challenges.

India, with its 860 million mobile subscriptions (although, the numbers of users would be lower than this figure) is looking more and more to the internet as a delivery platform of socio-economic programs and a tool to boost the economy. That the internet can raise GDP by 10% is a much favoured figure for those who promote the internet for economic reasons. The fact is that as the remaining unconnected population of India begins to acquire net connections through desktops and smart phones, the government is increasingly looking at security and surveillance over the internet as a necessary and inevitable route. This also means that the government needs to rely on industry to help them with this gigantic task[11].

According to the internet crime report[7] for the year 2012, India ranks number 5 in terms of the numbers of the victim complaints.

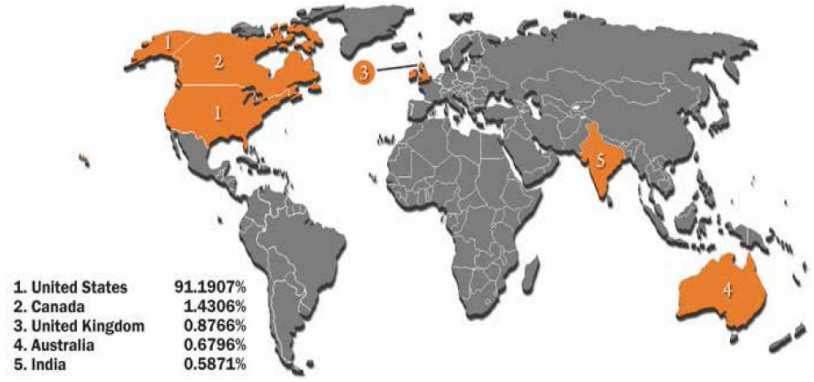

Fig 4 Top 5 Countries by Count: Victim Complainants (Numbered by Rank) [7]

The first line of defence against any cyber threat is increasing perception and awareness of cybercrimes. The organization facing cyber attack not only faces financial loss, but also loss of reputation, data loss etc. Based on the survey conducted by KMPG on Indian Industries[13], some of the major concerns of organisations that are victims of a cyber attack incident are presented in the figure below.

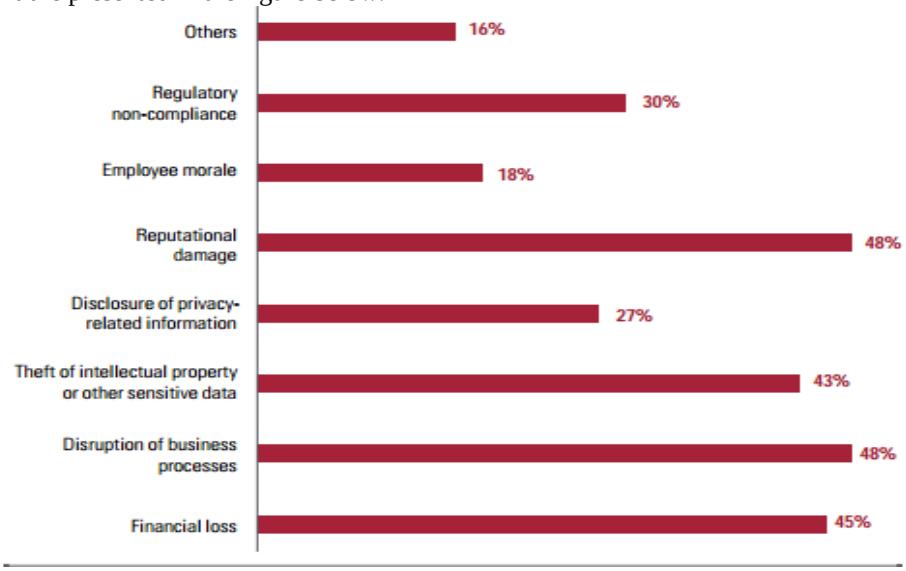

Fig 5 Impact of Cybercrime in India [13]

One of the best ways to do tackle this menace is through education and security awareness. No matter how great security tools are, the human beings using the devices, typing on the keyboard, and clicking the mouse are the weakest link. User error can torpedo even the best defence[4]. One of the main reasons for increase in cyber crime is lack of awareness; hence, people need to be educated on a large scale. The continuous development of information and communications technologies (ICT) is one of the drivers of the knowledge economy. Technology continues to gain ground in higher education and has already enhanced the on-campus student experience through student portals, Internet access, digital libraries and availability of laptops, handhelds and other portable devices . E-learning is becoming part of the mainstream of educational programmes [17].

The use of Open Education Resources (OER) to facilitate the efficient creation, distribution and use of knowledge and information is another recent innovation. Massive Open Online Courses (MOOCs) can be used as a means of facilitating the efficient creation, distribution and use of knowledge and information for learning. MOOCs have no prerequisite courses and no formal accreditation — anyone can participate online[21]. Coursera co-founder Daphne Koller has played up the unprecedented reach of online education, particularly to underserved demographics, making the case that MOOCs may bring world class education to those who are otherwise excluded for socioeconomic or geographic reasons[6]. The MOOC movement started in 2008 when George Siemens, Stephen Downes and David Cormier created a MOOC on Connectivism and Connective Knowledge 2008(CCK08). It was followed by Sebastian Thrun and Peter Norvig who launched a MOOCs based course on Artificial Intelligence at Stanford in 2011. The course received an overwhelming response and more than 170000 people registered for the course from all over the world. This motivated them to start a company called Udacity in the year 2012 after quiting their jobs at Stanford. Soon after, in April 2012, Daphne Koller and Andrew Ng, both Stanford colleagues involved in the Stanford MOOCs, started Coursera. In May, Harvard and MIT joined together to create the EdX platform. Since then many universities have joined the xMOOCs bandwagon globally (including the IITs from India), and many new MOOC initiatives have sprung up rapidly across the world such as Udemy, P2PU, FutureLearn, OpenStudy and Canvas. IIT Delhi and BITS Pilani are offering courses (using Coursera) to their own students[10].

Implemented properly, the massive and cost effective nature of MOOCs can provide a solution to the problem under consideration and can be used to spread cyber security awareness among youth. The massive nature of MOOC ensures the benefit can be availed by large numbers. More the number of students, more the benefits of collaborative learning[5]. The only effective way to address security issues is to be prepared for them; therefore, creating awareness about the cyber security to the masses in the large scale using MOOC is the need of an hour.

REFERENCES

[1] Anand, J. (2012). *Delhi registered 1850% rise in cyber crime cases.* The Hindustan Times dated 08 July, 2012.

[2] Athavale, D. (2014). *Cyberattacks on the rise in India.* The Times of India dated 10 March, 2014.

[3] Bhargava, Y. (2015 , Aug. 08). *India follows global trends in taking on cyber attacks*. Retrieved Dec. 17, 2015, from http://www.thehindu.com/news/national/india-follows-global-trends-in-taking-on-cyber-attacks/article7513800.ece

[4] Bradley, T. (2013). *Awareness, User Education Most Effective to Beat Cybercrime.* CIO.

[5] Devgun, P. (2013). Prospects for Success of MOOC in Higher Education in India. *International Journal of Information and Computation Technology , 3* (7), 641-646.

[6] Garcia, L. N. (2014). *The End of MOOCS and the Future of Education.* The UBYSSEY.
[7] IC3. (2013). *Internet Crime Report-2012.* Internet Crime Complaint Center.
[8] Indian Express. (2014). *IIT Bombay launches its first MOOC courses on the edX platform.* New Delhi: Indian Express dated 14 may 2014.
[9] Information Week. (2013). *91 percent of organizations suffered a cyber-attack in 2013: Survey.* Information Week dated 12 Dec. 2013.
[10] Jain, B. N., Gopalakrishnan, G., Mehra, L., Kannegal, M., Upadhyay, M., Pankaj, R., et al. (2014). *MOOCS and the Future of Indian Higher Education.* FICCI.
[11] Kaul, M. (2013). *India challenges cyber governance and security.* http://www.indexoncensorship.org/2013/10/india-challenges-cyber-governance-cyber-security/.
[12] KMPG. (2011). *Cyber Crime – A Growing Challenge for Governments.* KMPG International.
[13] KMPG. (2014). *Cyber Crime Survey Report 2014.* KPMG INTERNATIONAL.
[14] McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence.* Home Office Research Report 75 .
[15] National Crime Records Bureau. (2013). *Crimes in India 2013 Statistics.* National Crime Records Bureau, Ministry of Home Affairs, Govt. of India.
[16] New Indian Express. (2014). *India 7th in Cyber Attacks, 85th in Net Connectivity: Report.* New Indian Express dated 01 July 2014.
[17] OECD. (2007). *Giving Knowledge for Free: THE EMERGENCE OF OPEN EDUCATION RESOURCES.* Center for Educational Research and Innovation. ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT.
[18] Paolo, P. (2014). *August 2014 Cyber Attacks Statistics.* http://hackmageddon.com/category/security/cyber-attacks-statistics/.
[19] *PTI*. (2015, Dec. 02). Retrieved Dec. 17, 2015, from http://www.ndtv.com/india-news/54-483-cyber-security-incidents-reported-this-fiscal-year-government-1250244
[20] PTI. (2014). *India second on cyber attacks on mobile.* The Indian Express dated 2 March, 2014.
[21] Rory McGreal, Wanjira Kinuthia and Stewart Marshall. (2013). *Open Educational Resources: Innovation, Research and Practice.* Vancouver: Commonwealth of Learning and Athabasca University.
[22] Singh, G., Sharma, A., Rampal, K., Kular, R., Gupta, S., Sarita, R., et al. (2013). *India Risk Survey 2013.* Pinkerton and Federation of Indian Chambers of Commerce and Industry (FICCI).
[23] *The Telegraph*. (2015, Dec. 06). Retrieved Dec. 17, 2015, from http://www.telegraphindia.com/1151207/jsp/business/story_57045.jsp#.VnJcINJ95dg
[24] Verma, A. K., & Sharma, A. K. (2014). Cyber Security Issues and Recommendations. *International Journal of Advanced Research in Computer Science and Software Engineering , 4* (4), 629-635.
[25] Joshi, S. (2013). An IT superpower, India has just 556 cyber security experts. Retrieved Jan. 14, 2014, from http://www.thehindu.com/news/national/an-it-superpower-india-has-just-556-cyber-security-experts/article4827644.ece
[26] Sen, A. (2013, June 15). EU not ready to give India 'data secure' status. Retrieved Jan. 16, 2014, from The Hindu: http://www.thehindubusinessline.com/info-tech/eu-not-ready-to-give-india-data-secure-status/article4817820.ece

