Need to understand Cyber Crime's Impact over national Security in India: A case study

P.R. Patil and D.V. Bhosale
Dept. of Defence & Strategic Studies, Tuljaram Chaturchand College, Baramati, Dist-Pune, Maharashtra, India

Abstract

This Study focuses on how cyber crime is significant enough to become national security priority and how environment in India is vulnerable for cyber attack. This vulnerable environment can exploit by the hacker and may be that will be any national security issue all over the country. Information is powerful tool in today's planet. This paper addresses the cyber threats and the awareness of the people regarding the same. Through interviews of student, Teachers (of computer science), Bank Employees, Information Security Professionals this paper aims to identify the current scenario of cyber crime and how it can affect national security of India. Our finding shows that Indian people don't have much awareness about the cyber crime and this can be harmful for national Security. To mitigate these risks we have provided solutions and suggestion it can reduce the impact of cyber crime.

KEYWORD: - Need of e-society, Problem for e-society, Impact of e-society's problem over national security.

Introduction: -

Today's world is known as w^3 (World Wide Web) planet. Computer Network is backbone of growth of economies, vigorous research communities, strong militaries, transparent governments, and faire free societies. The electronic services like emails, internet banking & cyber space are essential part of society. So, Cyber security and information security are growing demands across all the sectors in the government as well as private firms. With the advent of information technology comes a threat of it is being misused. Today cyber crimes are much more sophisticated than they were saying 5 years back [(1)]. Cyber attacks pose serious threats to the sensitive information, possessed both by public and private sector, and could potentially jeopardize national security [(2)]. Cyber crime is threat to National Security of all countries [(3)]. We hear about viruses causing millions of dollars damage, hackers from other countries capturing credit card information from financial institutions, websites of large corporations and governments being defected for political reasons. This happens with technologically developed countries also. But in India Environment is little bit different because most of the people don't even know that anybody can still their important information about credit card or internet banking. So there is need to aware those people, how this problem is becoming global issue. Cyber crimes reported in India are Denial of Service, defacement of website, Spam, Computer virus and worms, pornography, cyber squatting, cyber stalking and phishing[(4)].

When we see the history of world we come across, there is a negative thinking mindset is rises the critical environment in front of society. As a resultant jeopardize national security comes in crucial. Lot of thinker think over it and tries to provide solution on it and lot times it will be change his face. Now it comes in front of world in the scene of cyber-crime and cyber-terrorism—increasingly intruding into today environment. Before starting the discussion we have to know that what is cybercrime and types of cybercrime. "Any crime that happens through the computer or computer network is called as cybercrime." There are various types of cybercrimes noticed a)Financial crime b) Cyber pornography c) IP crime d) Email spoofing e)Cyber Stalking f) Unauthorized Access (Hacking) h) Email bombing i) Salami Attacks j) Virus and worms k) Denial of service (DOS) attack l) Cyber terrorism m) Trojan attacks(5).

Cyber threats are currently significant enough to become a national security priority all over world. Today's main formula is "Information is power". Without using any weapon cybercrime can impact more dangerously on national security. Cybercrime is equally dangerous like cyber war and both can impact on security services like Army, navy and air force. If attacker push any bug in air force system it can be dangerous. Attacker also gains confidential data or information about Missile program of country. The C3 (Command, Control, Communication) term is most important from angel of defence forces. Now days this happens through satellite or wireless networks. If any malicious person gets control of this system, it can be harmful to national security. As corresponding to this issue Government of India should pay attention on this issue because last two incident happened in the country are very serious first incident is Pakistani group of hackers defected the Bhabha Atomic Research Center Website just after India's May 1998 nuclear test, and II) MPSC (Maharashtra Public Service Commission) server got crashed due to virus attack. The exam was to be conducted for 3.5 lack candidates to fill up 265 posts of class 1 and 2officers, but with the data lost the MPSC unable to conduct the exam(6). These two issues are indicating how cybercrimes affect the national security. India also observed a significant increase in the number of cyber security attacks on vital installations and key government ministries like PMO, External Affairs, Home Ministry, etc. A total of 8,266, 10,315 and 13,301 security incidents were reported to and handled by Cert-In during 2009, 2010 and 2011, respectively. India has also become a target for cyber espionage. Over 250 Indian websites including the Ministry of Defence, Ministry of Railways and several Indian missions abroad have been attacked in the recent past(2). Given facts nearly $ 120 million worth mobiles are being lost or stolen in the country every year the information or contact details these could be misused(4).

Now days Chinese hacker become headache for world these hackers have stolen most confidential information of countries like America, Australia, Brittan, and India (7). Resent news shows that Chinese hackers have stolen Blue print of Black Hock helicopter, Patriot missile and Washington post is also agreed with this(8). These Countries are more advance in communications as well as information technology than India. These countries also suffering from this issue then India needs immediate attention on this global issue.

Methodology: -

In the present work, the questionnaires are used for different sectors like a) Education b) Banking c) Information Security Professionals. In the education sector, the students and teachers of computer science are assessed for their knowledge of cybercrime. The Samples are of different age group from 16 to 50 yrs. The questionnaires prepared are given to the stakeholders of different sectors and data was collected (The questionnaires for each sector is attached as annexure). The data was processed 20 samples from each sector was used together as source of information.

Result and Analysis:-

In the present work, the different questions are used for different Sector's like a) Education b) Banking c) Information Security professional from IT sectors. In the education sectors, the students and teachers are assessed for their knowledge of cybercrime. The samples are different age group from 16 to 50 yrs. 20 samples are from age group of 16 to 20 and all are college students. This group of students now a day continuously in touch with the internet and use of net for learning is routine practice of students. But in this survey it is observed that even though the students are use to with internet they are not well aware about the cybercrime. Among the students 57% of students don't know that the use of pirated software is cybercrime. Most of them (67%) receive spam mail but only 4% respond to them. We have asked some questions regarding the access of pornographic website. The students are not aware about the fact that use and distribution of porn is under cybercrime. Around 77% students use Bluetooth for transfer of data. On the other hand it is interesting to note that, most of the students never face the form of cybercrime, or they may don't have more information about the forms of cybercrime, only spam mail or junk mail is the problem in front of these students. Use of piracy is again common in students.

In the second part, we have analyzed the college teachers. 100% of them are regular net users and 80% of them are aware about the cybercrime. But 50% of them well known about the origin of cybercrime. It interesting to note here that, from the teachers 60% do not know that using pirated software is cyber crime. 90% of them receive spam mail but nobody respond to them. 80% teachers do not know that access of pornographic website or its distribution is comes under cybercrime. They are use to with Bluetooth and 80% of them transfer data through Bluetooth. About 70-80% of teachers do not face any type of cybercrime. Spam mail is again common problem for teachers.

Financial Sector is the most important group who is under tremendous threat of cybercrime now days the Banking sector introduces online banking for beat and easy access of account to the customers. But the use of online banking becomes dangerous. There are several using like hacking of ATM cards, gathering of customer accounts information by spam mail or transfer of funds from their accounts, online transfer of money from other account etc.

To know the issues and present status of cybercrime in the banking sector, we have assessed the personals working in the banks. From them 90% are regular Net users and knows about the cybercrime. But unfortunately, 60% of them do not know the types

of it , and how it take place 40% of them use pirated software's and 80% are not aware that use of pirated software is cybercrime , 90% receive spam mail and they never respond to them.

It is interesting to note here that 70% of bank employee does not know how to secure the data and information that they have, and even the bank does not provide any training about the information security. Most of the banks employees (80-100%) never face the form of cybercrime excluding the spam and junk mail.

We have assessed information security professional with different age group and profession. Basically all of them know the cybercrime and its types. They very frequently face the spam/junk mails. On an average they face the DOS, Salami attacks, cyber stalking, cyber harassment, phishing is frequent for them. Above 70% professionals face the phishing and cyber stalking.

Suggestions or Solutions:-

We have analyzed Information Security professional's opinions about the impact of cybercrime on national security, according to them

1) The internet revolution has brought the world together which huge dependency of the public is in the network and the information hosted over a public channel is vulnerable to cyber attacks. As government bringing the basic services such as electricity, gas etc. online, it is necessary to protect these services from cyber attack.
2) To secure computer network around us, it is essential to aware the users as well as use some traditional methods like use of firewall, proxy, IDS, antivirus software. Technologies are also available but it has limitation and requires continuous updating
3) Our one question related with the needs of study on information security, the opinion was in India, the information security awareness is not as evident as foreign countries like US, or Europe
4) The scarcity of skilled information security professionals has created a huge gap and requires immediate attention. Defence, Banking, Research and development, private sectors, BSE, NSE should be on prime focus. Cyber laws education new paradigm for controlling the cyber attacks.
5) Therefore by knowing the present status, it is now essential to bring awareness among the stakeholder.

Conclusion: -

1) Every individual of the country has some part of information and that information may secure. An important same for the cyber criminals the way presents who can be protected from cybercrime may be from simple and single spam/junk mail or even from the terrorists.
2) In India information security training should provide from college level so we can assemble skilled persons to right post and gap of information security professionals will be fulfilled

3) Recent incidents indicate that Indian people don't have awareness about cybercrime. So it requires awareness among the people who use internet and internet banking regarding the cyber crime or cyber fraud. Banks should organize campaign by that they can train the costumers about online services and cybercrime.
4) To face the cyber crime and cyber war government can start cyber army or separate unit that will be take care of only cyber crimes and cyber attacks. And also that unit can help to Government for applying cyber laws.

This piece of work is only initiative and further the work will be extended at state level. The work on collection of information at large scale is under progress.

Reference: -

1) Elect news networks(ENN) April1, 2011 (India in need of dedicated cyber security policy)
2) Elect news networks(ENN) April5, 2013 (A Proposed National Policy on Information Security in India)
3) Peterson, O. M. Gladys, M. O. and Christopher, J. I.(2011)"Effects of cyber crime on state security: Types impact and mitigations with the fiber optic deployment in Kenya" Journal of Information Assurance & Cyber security Vol.2011
4) The Hindu News on 27 oct 2007
5) Connolly, C. (2009) "Cyber law," Hot Topics: Legal Issues In Plain Language, No. 70, State Library of NSW. http://www.legalanswers.sl.nsw.gov.au/hot_topics/pdf/cyberlaw_70.pdf
6) Jai Maharashtra News | 03 Apr Wed, 2013
7) Sakal News Paper | 22 June Sat, 2013
8) Tej News | 31 May Fri, 2013.