Suresh Gyan Vihar University,
Jaipur International Journal of Converging Technologies and Management (IJCTM)
Volume 1, Issue 2, 2015
ISSN : 2455-7528

A Value Creation Approach towards cyber safety mechanism: Analysis and Evaluation

Raksha Chouhan

Abstract :- Internet based global fraud rate is increasing rapidly and there is a potential impact of cyber crime on quality production time, overhead cost, economy, market value as well as on consumer trust. Cyber space is used for violating copyright, trafficking in human organs and prohibited drugs, violating individual's privacy, pornography, gambling, hacking, terrorism, money laundering, fraud, software piracy and corporate surveillance etc. Thus Growing danger from crimes committed against electronic information on computers is alerting us to claim attention in national capitals and dedicated legislation on cyber crime to supplement the Indian Penal Code is demand of the state of art. The objective of this research paper is to critically analyze cyber safety mechanism and trends to protect our society and to crack as to how the issue of cyber crimes has been dealt with in our society. This paper also examines the reasons behind failure of legal mechanism and also identifies the methods by which cyber crime can be reduced.

KEYWORDS: Cyber Attacks, Cyber Crimes, Cyber Law, I.T.A. 2000, ITAA 2008, Information Technology and National Security etc.

Faculty, Prestige Institute of Management and Research, Indore (Madhya Pradesh)
E-mail: rspardeshi30@gmail.com, raksha_chauhan@pimrindore.ac.in

1. Introduction

Cybercrime is an activity performed by criminal by using an element of a computer or network of computers. According to an Assoc ham-Mahindra SSG study "The number of cyber crimes in the country may double to 3 lakh in 2015 and could pose serious economic and national security challenges" [4]. According to Computer Emergency Response Team-India (CERT-In) report till May 2014 total 9, 9,174 Indian websites were hacked by hacker groups spread across the world [5]. Methods of attack are becoming even more sophisticated with the passage of time. It has become one of the most serious economic and national security threats. It has affected almost every area including

defense, medical, computer infrastructure, transportation, defense etc. Confidentiality, integrity with reference to quality, accuracy and relevance and availability are major role playing factors towards cyber security. A threat can be defined as a potential danger to information and system. Three levels of cyber threat have been shown below [1]:

Unstructured Threats	**Structured Threats**	**Highly Structured Threats**
Individual/small group with little or no organization or funding	Well organized, planned and funded	Extensive organization, funding and planning over an extended time, with goal of having an effect beyond the data or machine being attacked
Easily detectable information gathering	Specific targets and extensive information gathering to choose avenue and means of attack	Stealthy information gathering
Exploitations based upon documented flaws	Goal-data stored on machines or machines themselves	Multiple attacks
Targets of opportunity	Exploitation may rely on insider help of unknown flaw	exploiting unknown flaws or insider help
Gain control of machines	Target drives attack	Coordinated efforts from multiple groups
Motivated by bragging rights, thrills, access to resources	Organized crime/black hat hackers	"Cyber warfare"

Table 1: Different Levels of Cyber Threat

Top-Ten Types of Information violated by hackers in 2013 are-Real Names, Birth Dates, Government ID Numbers (Social Security), Home Address, Medical Records, Phone Numbers, Financial Information, Email Addresses, User Names & Passwords and Insurance. Top-Ten Industries Targeted in Spear-Phishing Attacks in 2013 are Public Administration (Gov.), Services – Professional, Services

– Non-Traditional, Manufacturing Finance, Insurance & Real Estate, Transportation, Gas, Communications and Electric, Wholesale, Retail, Mining, Construction. In the following chart total number of vulnerabilities from 2006 to 2013 has been shown [2]:

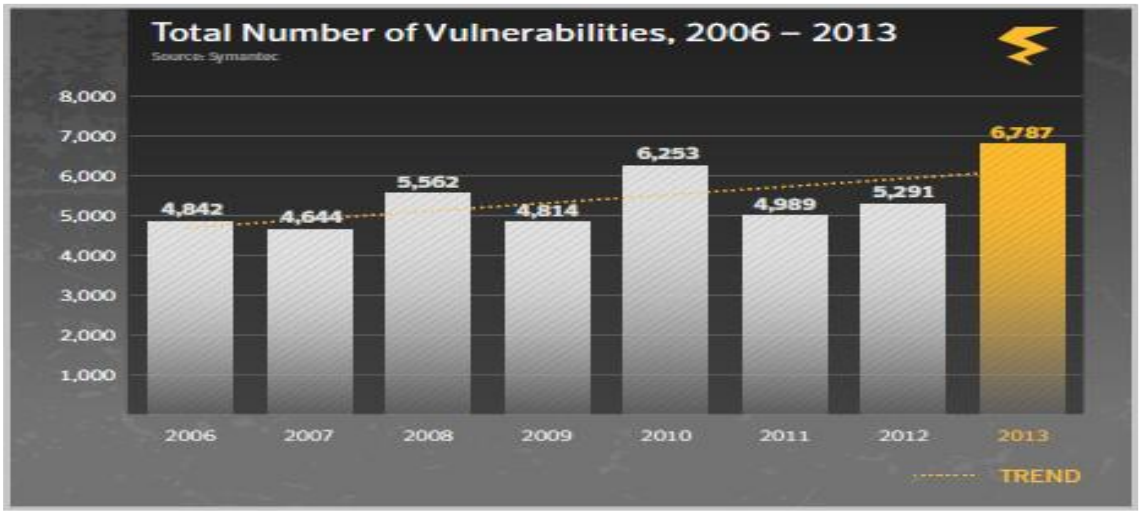

Fig 1: Total number of vulnerabilities from 2006 to 2013

Fig 2 is showing various stages of cyber attack evolution from year 1980 to the year 2000+ [3]:

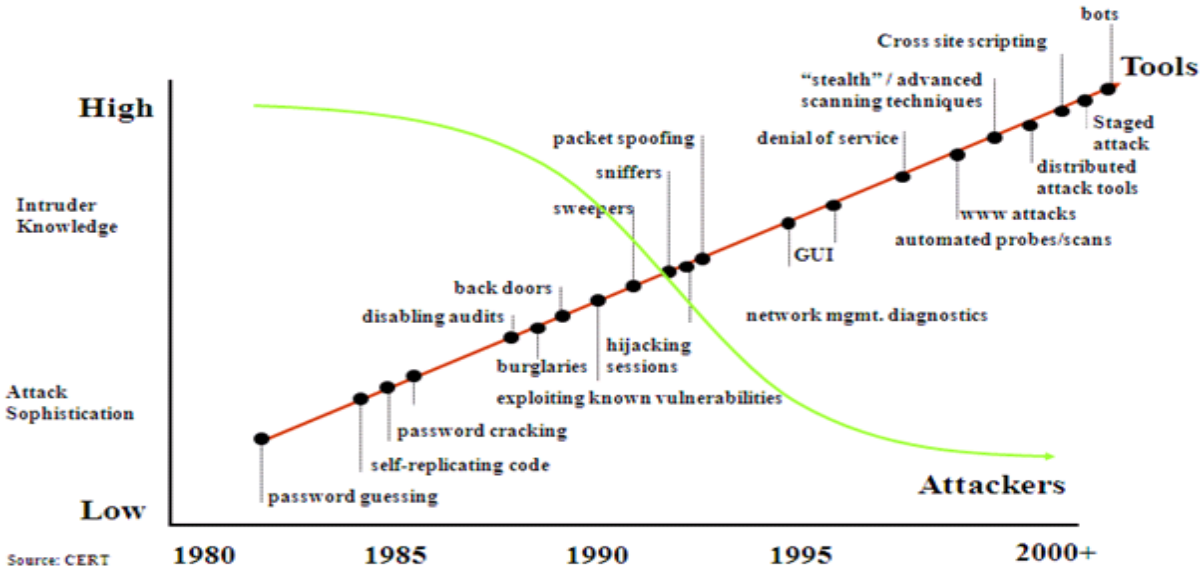

Fig 2: Various stages of cyber attack evolution

2. Objectives of the Study

1. To critically analyze emerging trends for cyber safety mechanism to protect our society.

2. To analyze the reasons behind failure of legal mechanism.
3. To identify the methods by which cyber crime can be reduced for the betterment of the society.
4. To find out various initiatives taken by international and national organizations towards cyber safety mechanism.

3. Methodology

All most every area like income tax, passport visa has been intensely involver in E-governance and now India is shifting gears towards E-governance. In this study a systematic review on cyber crime as well as upcoming trend used for cyber safety mechanism has been done. The study is focused on a safety mechanism and tries to identify, appraise, select and synthesize all high quality research evidence relevant to the matter. A combination of existing literature studies and in-depth secondary database material is used to fulfill the objective and the material has been referred from Online as well as desk based book reviews, articles, reports, research and conference papers.

4. Most pervasive cyber crime schemes and reasons responsible for growth in cyber crime

Cyber Crime is on the increase and a lack of awareness, and inappropriate, limited or absent countermeasures have only aggravated the negative impact of e-fraud on society. Most pervasive cyber crime schemes are Internet auctions and retail schemes, Internet business opportunity schemes, Internet work-at-home schemes, Internet identity theft schemes, Internet investment schemes, Internet effortless income schemes, Internet free goods schemes, Internet health and diet schemes, Internet guaranteed loans or credit, on easy terms schemes, Internet credit repair schemes, Internet vacation prize promotions schemes, Internet 'quick divorce' scheme and Salami Techniques etc whereas reasons responsible for growth in cyber crime are[6]:

1. 24X7 worldwide connectivity.
2. Increasing complexity of computer software
3. Availability of malicious code and tools in large quantity.
4. Demanding pace of technological change.
5. Slow adoption rate of good computer security practices

5. Counter Measures used to provide cyber safety mechanism

The most popular weapon in cyber terrorism is the use of computer viruses and worms. Antivirus stays helpless until and unless its database is updated periodically to discover new attacks like hijacking, Denial of Service etc. therefore other software's are also needed along with the use of antivirus. It is good practice not to eliminate the firewall from our system even if it has limited capacities compared to IPS or IDS, because a firewall reduces the amount of the bad traffic that can reach the IPS and IDS, which will reduce the alarms and the suspicious data. Following are some Counter measures and cyber safety Mechanism used in current scenario [7] [8] [9]:

A. Intrusion Detection System (IDS): Any group of actions that attempt to compromise the integrity, confidentiality and availability of information is called as an intrusion. Hence Intrusion detection is considered as an additional wall to protect systems and it is useful not only in detecting successful intrusions, but also provides important information for timely countermeasures. Thus Intrusion Detection System is used to monitor events occurring in a computer system or network and analyzing these occurrences which may violate safety mechanism. The alarm of IDS is launched when an intrusion / interference have break in/enter the system. There are two types of IDS: HIDS and NIDS. HIDS is more reliable way as compare to NIDS because it can detect illegal access easily but at the same time HIDS delivers all the collected information to a central computer. This means that in an internal network if we have a big number of machines with HIDS then it may be risky because big flow of information could diminish the performance of the system, that's why NIDS is preferred in that kind of network even that he could miss some illegal access that HIDS can see.

B. Intrusion Prevention System (IPS): We need something that prevents the attacks before it happens. IPS identifies and stops the malicious codes before they penetrate in our system; this type of software's provides the 4'h layer of protection shield to the system.

An intrusion detection and prevention system (IDPS) identifies possible incidents and their logging information, attempt to stop them, and generate a report to the security administrators. IDPS also used to identify problems with security policies and to documents existing threats. They use several response techniques, which involve the IDPS in stopping the attack itself, changes the security environment like by reconfiguring a firewall or changing the attack's Content etc.

C. Distributed Intrusion Detection System (DIDS): DIDS are superset of the conventional IDS, implemented in a distributed environment. In DIDS, conventional IDS are fixed inside intelligent agents and are installed on a large network. In a distributed environment, IDS agents communicate with each other, or with a central server. Distributed monitoring allows early detection of planned and coordinated attacks and in this way allows network administrators to take preventive measures. DIDS also assists to control the spreading of worms, improves network monitoring, incident analysis, attack tracing etc. It also helps to detect new threats from unauthorized users, backdoor attackers and hackers to the network across geographically separated locations.

D. Agent Based Distributed Intrusion Detection System (ABDIDS): Agent based distributed Intrusion detection system is an essential factor of protective measures to protect computer systems and networks from exploitation. It is a fully distributed system and automates security management tasks. It is made by set of nodes with three types of agents: Monitoring Registry Agents (MoRA), Monitoring Agents (MoA) and managing agents (MA). Besides other functionalities of IDS it provides facilities like early warning when pre-attack activities are detected as well as detecting and isolating compromised nodes by trust mechanisms and voting-based peer-level protocols.

E. GPRS Security Architecture: GPRS uses a set of security mechanisms that comprises the GPRS security architecture. Most of these mechanisms have been originally designed for GSM, but they have been modified to adapt to the packet oriented traffic nature and the GPRS network components also. Two main goals of GPRS security architecture are to protect the network against unauthorized access, and to protect the privacy of users. Components of GPRS are Subscriber Identity Module (SIM), Subscriber identity confidentiality, Subscriber identity authentication and GPRS backbone security.

6. Role of International / National Organizations towards Cyber Safety Mechanism

The economic growth of any nation and its security depends on how well is its cyberspace secured and protected. In recent cyber security measures Non Government (private) regulatory measures, National Law and enforcement measure, Defensive strategies, products as well as some limited forms of international cooperation and regulations plays important role. Some of the initiatives taken by

private and government (national/International) organizations are shown in the following table [7] [10]-

S. No.	Organization Name	Initiatives
1.	**Non Government Organization**	Several Non government entities play significant operational roles on aspects of cyber security.
a)	**IETF** Internet Engineering Task Force	IETF have developed and proposed some technical standards for the Internet including current and next-generation versions of the Internet Protocol.
b)	**Web Consortium House**	Situated at the Massachusetts Institute of Technology have defined technical standards for the web technology.
c)	**FIRST** (Forum of Incident Response and Security Teams)	FIRST tries to coordinate the activities of both government and private Computer Emergency Response Teams (―CERTs‖) and is also working on cyber security standards.
d)	**IEEE** (Institute of Electrical and Electronics Engineers)	IEEE develops technical standards through its Standards Association and in conjunction with the U.S. NIST (National Institute of Standards and Technology).
e)	**ICANN (**Internet Corporation for	

	Assigned Names and Numbers)	It operates pursuant to a contract with the U.S. Department of Commerce (September 2009) transferring to ICAAN the technical management of the Domain Name System.
2.	**Government Organization**	Governments of different nations have adopted laws with the intension of punishing to prevent specific forms of cyber attacks or exploitation but these laws have little or no effect.
a)	**DSCI** (Data Security Council of India)**:**	It is an organization established to promote data protection with two main objectives: one is to teach best practices to prevent attacks and another one is to help in capacity building to handle occurrences when attack happen.
b)	**NIC (**National Informatics Centre)	A premier organization providing network backbone and e-governance support to the Central Government, State Governments, Union Territories, Districts and other Governments bodies. It provides broad range of ICT services including nationwide communication Network for the purpose of centralized planning in Government services as well as to provide wider transparency of national and local governments.
c)	**Cert-In** (Indian Computer Emergency Response Team)	It is the most important constituent of India's cyber community. Its mandate states "ensure security of cyber space in the country by enhancing the security communications and information infrastructure, through proactive action and effective collaboration aimed at security incident prevention and response and security assurance".
d)	**NISAP (**National Information Security Assurance Program)	This is for Government and critical infrastructures, Highlights are :

		a) Government and critical infrastructures should have a security policy and create a point of contact. b) It is compulsory for organizations to implement security control and report any security incident to Cert-In. c) All Security obedience followed by the organizations should be reported periodically to Cert-In. A panel of auditor for IT security would be provided by Cert-In as and when needed and all organizations to be subject to a third party audit from this panel once a year.

3.	**International Organizations**	National governments often cooperate with each other informally by exchanging information, investigating attacks or crimes, preventing or stopping harmful conduct, providing evidence, and even organizing for the performance of individuals to a requesting state. States have also made formal, international agreements that bear directly or indirectly on cyber security. These agreements potentially bear upon cyber-security activities and also include universally accepted rules of conduct. International law also provides rules related to the use of force during armed conflicts that most probably apply to cyber attacks.
a)	**IUSCSF** (Indo-US Cyber Security Forum)	This forum was set up in 2001 and in this forum high power delegations from both side met and several initiatives were announced. Highlights are a) Setting up an **ISAC** (Information Sharing and Analysis Centre) for better cooperation in anti hacking measures. b) Setting up IABA (India Anti Bot Alliance) to raise awareness about the emerging threats in cyberspace by the CII (Confederation of Indian Industry). c) Ongoing cooperation between India's STQC (Standardization Testing and Quality Certification) and the US NIST (National Institute of Standards and Technology) would be expanded to new areas. d) The R&D group will work on the hard problems of cyber security, Cyber forensics and anti spasm research.

b)	**USNSE** (United State National Security Experts)	e) Chalked the way for rising mutual cooperation to control cyber crime between the two countries. US NSE have recommended: i) National laws to protect information sharing from various threats and attacks. ii) Methods for government bodies to cooperate with private entities in evaluating the source and nature of cyber attacks like NSA. iii) Development of more effective cyber security plans through government-sponsored research and coordination towards cyber attacks and exploitation.

Table 9: Initiatives taken by private and government (national/International) organizations

7. Conclusion

Online communication has become essential in digital age and as a result cyber crime has emerged as a very concrete threat. It is committed by technocrats and the returns are enormous and the risks are stumpy. In present scenario India is actually aware about its reputation because of the critical position of cybercrime where foreign investors can do business and has been investing heavily in cyber security.

One key to get better cyber security is an enhanced understanding of the threat and of the vectors used by the attacker to hijack important information. Implementation of a more methodological approach is required to freeze security. There are a variety of frameworks that can help, and each one may suit different organizations in different ways. Businesses and organization should adapt, use and maintain standard framework to fight with emerging threats and challenges. Some critical control protection priorities have been discussed below: [2]

1. Unauthorized and unprotected system including servers, workstations, laptops etc connected to the enterprise network should be monitored and configured properly to avoid exploitation.

2. Inventory should be maintained and only necessary and authorized software's should be installed to reduce attacks.

3. Easy access through networks and browsers should be prevented and Secure Hardware & Software Configurations should be deployed and regularly updated.

4. Automated antivirus and anti-spyware software should be used to continuously monitor and protect workstations, servers, and mobile devices and they should be updated regularly and vulnerability should be repair quickly.

5. Web application firewalls should be deployed to inspect all traffic, and errors should be checked explicitly for all user input (including by size and data type).

6. Restoration process should be regularly tested and backup should be taken regular basis to minimize damages from an attack.

7. Knowledge gaps should be identified properly and initiatives should be taken to fill these gaps by skillful training programs.

8. Secure and standard Configurations for network devices such as Firewalls, Routers, and Switches should be used to prevent systems.

9. Use of administrative licenses should be controlled to protect and validate an administrative account.

10. Multi-layered boundary defense control should be established to control the flow of traffic.

Society as on today is happening more and more dependent upon technology and crime based on electronic offences are bound to increase. In the coming future new technology is going to provide broader opportunities for criminal by providing easier access to systems, premises, goods and information, and due to unlimited geographical coverage. The cost of cyber crime will continue to increase with the increasing functionality on internet of business organizations. The main challenge now for India is to train and equip its law enforcement agencies and judiciary, particularly outside big city like Delhi, Mumbai and Bangalore Government need to begin serious, methodical effort to collect and publish data on cyber crime so that countries and companies can make better choice for risk and policy.

8. References

1. Amelia Muccio (April 13, 2011)"Introduction to Cyber security & Information Assurance for FQHCs" Director of Emergency Management, amuccio@njpca.org,visited on 17-3-15.
2. Symantec Corporation, Internet Security Threat Report 2014:: Volume 19 2013 Trends, Volume 19, Published April 2014, PP 98, www.symantec.com.
3. Lance James CTO, (July 2005), "Phishing an evolution", company confidential, secure science corporation Secure Science Corporation 7770 Regents Rd., Suite 113-535, San Diego, CA. 92122-1967, (877)570-0455, http://www.securescience.net.
4. The Economic Times (Jan 5, 2015) "Cyber crimes in India likely to double to 3 lakh in 2015:Report",http://articles.economictimes.indiatimes.com/2015-01-05/news/57705670_1_cyber-crimes-online-banking-pin-and-account-number.
5. Computer Emergency Response Team-India (CERT-In) reports 62,189 cyber attacks till May 2014, http://www.techmistory.com/2014/07/cert-in-reports-62189-cyber-attacks.html, visited: 10-1-15.
6. Dr Hugh McDermott (visited: 24-1-15), Cyber Crime – Present and Future Trends Director, AML-CTF, Fraud & Financial Crime Program, Australian Graduate School of Policing, Charles Strut University, pp 52.
7. Atul M. Tonge, Suraj S. Kasture , Surbhi R. Chaudhari(2013), "Cyber security: challenges for society- literature review", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-

0661, p- ISSN: 2278-8727Volume 12, Issue 2 (May. - Jun. 2013), PP 67-75
www.iosrjournals.org.

8. Janhavi J Deshmukh and Surbhi R Chaudhari (April' 2014), Cyber crime in Indian scenario – a literature snapshot, International Journal of Conceptions on Computing and Information Technology, Vol.2, Issue 2, pp 24-29, ISSN: 2345 – 9808.
9. Baroudi Siba, Ziade Haissam, Mounla Bassem (2004), "Are we really protected against hackers?" Proceddings International Conference on Information and Communication Technologies: from theory to application. PP. 621-622. IEEE
10. Col S S Raghav (visited: 28-11-14), "cyber security in india's counter terrorism strategy", pp 5, ids.nic.in.

----------x----------