Volume 4, Issue 4, April 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Cyber Security Issues and Recommendations

Anoop Kumar Verma
Department of Computer Science
Himachal Pradesh University Shimla, India

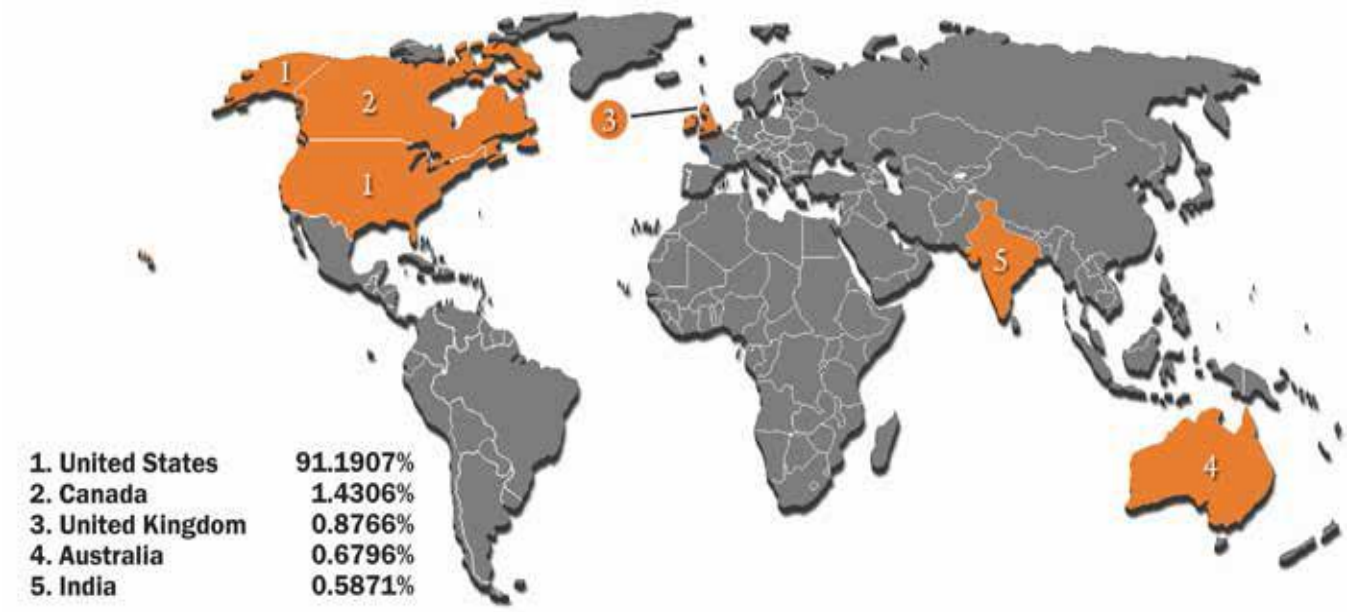
Aman Kumar Sharma
Associate Professor, Department of Computer Science
Himachal Pradesh University Shimla, India

Abstract— Cyber Security is of major concern in today's era of computing to secure data, network resources, and other critical information of an organization. This paper presents introduction to cyber security and the various threats to the cyber security and how these threats can be resolved. This paper also describes the various challenges of cyber security in India and Internet crime evolving around the world. Cyber security is now not restricted only to usage of Internet on a Desktop PC but securing information on Tablets, smart phones as they became very important communication medium because of technological advancements grown up very rapidly in past few years. To resolve issues related to cyber security the community of security researchers- including academia, the private sector and government sector must work together to understand the emerging threats to the computing world.

Keywords— Cyber Security, Cyber Crime, IC3 (Internet Crime Complaint Centre), CERT-In (Computer Emergency Response Team India), ISTF (Inter Departmental Information Security Task Force)

I. INTRODUCTION

Due to lack of information security various cyber crimes arises, "Cyber security" means set of activities, technical and non-technical aspects of protecting information, devices, computer resources, network resources and other critical information stored there in from unauthorized access, modification and disruption, disclosure [1]. According to emerging cyber threat report 2014 of Georgia Institute of Technology mobile devices bring a new set of threats, including allowing malicious software an unparalleled look into victim's lives. While mobile platforms have largely been safe for consumers and businesses, researchers and attackers are finding ways around the ecosystems security [2]. Cyber threats are asymmetric because attacks may be perpetrated by the few upon the many, with little cost and resources [3]. So cyber security in Information technology is of major concern in today's world of computing. According to IC3 [4] report 2012 (Internet Crime Complaint Centre) an alliance between the National White Collar Crime Centre (NW3C) and Federal Bureau of Investigation (FBI) the top five countries by count in victim complaints as numbered by Rank) as follows.



(Fig 1.Top 5 Countries by Count: Victim Complainants (Numbered by Rank))

II. THE INDIAN CYBER SPACE

The rapid development of the Internet over the past decade appeared to have facilitated an increase in the incidents of Online attacks [5] In India National Informatics Centre's were setup in year 1975 to provide various IT related solutions to the government. There were three major networks were setup at that time [6].

(a) INDONET:- It connects IBM mainframes that made up India's computer infrastructure
(b) NIC NET: It a NIC Network for public organizations that connects Central government with the state, and district administrations.
(c) ERNET: - It is an Education Research Network to serve the academic and research communities.

Critical sectors such as Defense, Energy, Finance, Space, Telecommunication, Transport and other public services heavily depends on the network to relay data, for communication purpose and for commercial transactions. So these sectors have a large impact of using the Internet as a source of communication, and information according to National broadband plan the target for broadband is 160 million households by 2016 and the Networking index estimates that India's Internet traffic will grow nine-fold between now and 2015. Although the government has ambitious plan to raise cyber connectivity, ecommerce services and communication channel but at the same time the government should make strong policies regarding the cyber attacks and security. The government should make protection against critical information infrastructure through public private partnership (PPP).

Concluded from the data drawn from global stats [7] the major attack types are Hacktivism, cyber crime, cyber warfare and cyber espionage are displayed in a graph showing Attack Trends.

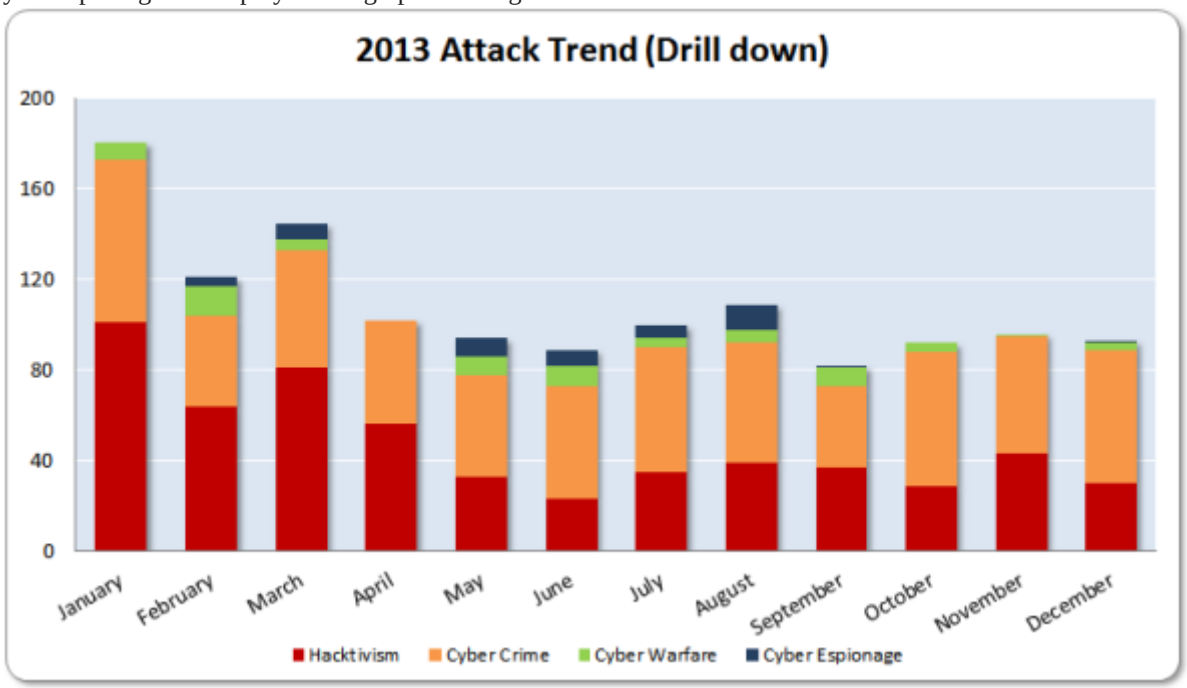


Fig. 2: Attack Trend

The following Table I shows Cyber crimes cases registered and persons arrested under IT Act during 2009 – 2012 at National Crime Records Bureau. Located at New Delhi at the attached office of Ministry of Home Affairs (MHA) [8]

TABLE I Cyber crimes/cases registered and persons arrested under IT Act during 2009 – 2012

Sr. No	Crime Heads	Cases Registered				% Variation in 2012 over 2011	Person Arrested				% Variation in 2012 over 2011
		2009	2010	2011	2012		2009	2010	2011	2012	
1	Tampering computer source documents	21	64	94	161	71.3	6	79	66	104	57.6
2	Hacking with computer system										
	I) Loss/damage to computer resource/utility	115	346	826	1,440	74.3	63	233	487	612	25.7
	II)Hacking	118	164	157	435	177.1	44	61	65	137	110.8
3	Obscene publication /transmission in electronic form	139	328	496	589	18.8	141	361	443	497	12.2

4	Failure										
	I) Of compliance/orders of certifying authority	3	2	6	6	0.0	6	5	4	4	0
	II) To assist in decrypting the information intercepted by govt. agency	0	0	3	3	0.0	0	0	0	3	-
5	Un-authorized access/attempt to access to protected computer system	7	3	5	3	-40.0	16	6	15	1	-93.3
6	Obtaining license or digital signature certificate by Misrepresentation/suppression of fact	1	9	6	6	0.0	1	4	0	5	-
7	Publishing false digital signature certificate	1	2	3	1	-66.7	0	2	1	0	-100.0
8	Fraud digital signature certificate	4	3	12	10	-16.7	6	4	8	3	-62.5
9	Breach of confidentiality/privacy	10	15	26	46	76.9	5	27	27	22	-18.5
10	Other	1	30	157	176	12.1	0	17	68	134	97.1
	Total	**420**	**966**	**1,791**	**2,876**	**60.0**	**228**	**779**	**1,184**	**1,522**	**28.5**

III. NATIONAL SECURITY POLICY 2013

India had no Cyber security policy before 2013. In 2013, *The Hindu*, citing documents leaked by NSA (National Security Agency) whistleblower Edward Snowden, has alleged that much of the NSA surveillance was focused on India's domestic politics and its strategic and commercial interests. This leads to spark furor among people. Under pressure, Government unveiled a National Cyber Security Policy 2013 on 2 July 2013 [9].

The Vision of the national security policy 2013 is to build a secure and resilient cyberspace for citizens, business and government. This policy is a proposed law by Department of Electronics and Information Technology, Government of India. Which is, aimed towards protecting the public and private infrastructure from cyber attacks. The policy also intends to safeguard "information, such as personal information (of web users), financial and banking information and sovereign data". This was particularly relevant in the wake of US National Security Agency (NSA) leaks that suggested the US government agencies are spying on Indian users, who have no legal or technical safeguards against it. Ministry of Communications and Information Technology (India) defines Cyber space is a complex environment consisting of interactions between people, software services supported by worldwide distribution of information and communication technology.

Ministry of Communications and Information Technology (India) define following objectives of the sated policy

1. To create a secure cyber ecosystem in the country, generate adequate trust and confidence in IT system and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy.
2. To create an assurance framework for design of security policies and promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (Product, process, technology & people).
3. To improve visibility of integrity of ICT products and services by establishing infrastructure for testing and validation of security of such product.
4. To provide fiscal benefit to businesses for adoption of standard security practices and processes.
5. To enable Protection of information while in process, handling, storage and transit so as to safeguard privacy of citizen's data and reducing economic losses due to cyber crime or data theft.
6. To enable effective prevention, investigation and prosecution of cybercrime and enhancement of low enforcement capabilities through appropriate legislative intervention.

Just days before the United Nation's led Internet Governance Forum in Indonesia, India, held its own – and first of its kind – conference on cyber governance and cyber security. With the support of the National Security Council Secretariat of the Government of India, the two-day conference was organized by private think-tank Observer Research Foundation and industry body, Federation of Indian Chambers of Commerce and Industry, (FICCI). Speakers were from a host of countries including Estonia, Germany, Belgium, Australia, Russia, Israel, and of course, India. There are two broad outcomes of this conference. The first is that India has indicated its willingness to start shouldering discussions to do with

the global cyberspace. The other is, as India's National Security Advisor put it, — "India has a national cyber security policy not a national cyber security strategy." This is certainly a start to building a consensus for that strategy. [10]

IV EXISTING COUNTER CYBER SECURITY INITIATIVES

Before looking into the security initiatives to be taken, look at the graph [7] showing various industries and government areas that interest the attackers for intrusion.

Fig.3: (Governments and Industries have been the most preferred targets for Cyber Attackers with similar values (respectively 23% and 22%). Targets belonging to finance rank at number three (7%), immediately ahead of News (6%) and Education (5%).)

So on the recommendations of ISTF [11] the following initiatives have been taken:

1) Indian Computer Emergency Response Team (CERT-In) has been established to respond to the cyber security incidents and take steps to prevent recurrence of the same.
2) Public Key Infrastructure (PKI) has been set up to support implementation of Information Technology Act and promotes use of Digital signatures.
3) Government has been supporting R&D activities through premier Academic and Public Sector Institutions in the country.

Some of the other initiatives that can be taken [12]

A. National Informatics Centre (NIC).

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 wide range of information and communication technology services including nationwide communication Network for decentralized planning improvement in Government services and wider transparency of national and local governments.

B. Indian Computer Emergency Response Team (Cert-In)

Cert-In 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

C. National Information Security Assurance Program (NISAP).

This is for Government and critical infrastructures, Highlights are [12]:

(a) Government and critical infrastructures should have a security policy and create a point of contact.
(b) Mandatory for organizations to implement security control and report any security incident to Cert-In.
(c) Cert-In to create a panel of auditor for IT security.
(d) All organizations to be subject to a third party audit from this panel once a year.
(e) Cert-In to be reported about security compliance on periodic basis by the organizations.

V RECOMMENDATIONS

A. Security Policy and Assurance

1) Critical sector can be protected by improvising the software development techniques and system engineering practices. In order to secure critical sectors more strengthened security models should be adopted.
2) Better training must be provided in order to assist users in IT security.

B. Early Detection and response

1) To avoid malicious cyberspace activities rapid identification and information exchange methods should be adopted.
2) Identification of key areas within the critical infrastructure.
3) Establish a public – private architecture for responding to national- level cyber incidents.

C. Security training and Programs

1) National awareness programs such as National Information Security Assurance Program (NISAP) need to be promoted.
2) Providing training and education programs to support the Nation's cyber security needs
3) Increasing the efficiency of existing cyber security programs and improving domain specific training programs (such as: Law Enforcement, Judiciary, and E – Governance etc).

D. Promotions and Publicity

1) In India we need to organize various workshop programs, conferences, and research programs in various IT institutes to enhance cyber security skills.
2) The promotion and publicity campaign could include seminars, exhibitions, contests, radio and TV programs, videos on specific topics, Web casts, Leaflets and posters, suggestion and award schemes.

E. Specific Recommendations [6]:-

1) Emphasis should be placed on developing and implementing standards and best practices in government functioning as well as in the private sector. Cyber security audits should be made compulsory for networked organizations. The standards should be enforced through a combination of regulation and incentives to industry.

2) The government should launch a National Mission in Cyber Forensics to facilitate prosecution of cyber criminals and cyber terrorists.

3) The impact of the emergence of new social networking media, and convergence of technologies on society including business, economy, national security should be studied with the help of relevant experts, including political scientists, sociologists, anthropologists, psychologists, and law enforcement experts. It should be ensured that the issues of privacy and human rights are not lost sight of and a proper balance between national security imperatives and human rights and privacy is maintained.

VI CONCLUSION

Although the government has ambitious plans to raise cyber connectivity. There has a boom in e-commerce, and many activities related to e-governance are now being carried out over the Internet. As we grow more dependent on the Internet for our daily life activities, we also become more vulnerable to any disruptions caused in and through cyberspace. The rapidity with which this sector has grown has meant that governments and private companies are still trying to figure out both the scope and meaning of security in cyberspace and apportioning responsibility.

The cyberspace holds the fifth place in common space and it is vital to have co ordinations and cooperation among all nations regarding cyberspace. The need of cyberspace and its exploitation is growing rapidly. The cyberspace is becoming important area for large number of terrorists to attack on crucial information infrastructure. The existing laws are inefficient to restrain the cyber crimes and, thus urging a need to modify the existing laws through which these activities can be put on a check. There is a need of international cooperation of nations to crack down the efficiency on cyber crime, thereby ensuring a development of the internet cybercrime is not limited to states of boundaries, thus it requires a universal collaboration of nations to work together to reduce the ever growing threats and risk to a manageable level.

REFERENCES

[1] Sunit Belapure, Nina Godbole, *Cyber Security*: *Understanding Cyber crimes, computer forensics and Legal Perspectives*, First Edition, Wiley India
[2] http://www.gtcybersecuritysummit.com/, "*Emerging Cyber Threats Report 2014*",[accessed on 6 March 2014 at 0900 hrs]
[3] asymmetricthreat.net/docs/asymmetric_threat_4_paper.pdf, "*Cyber Threats to National Security, Symposium One: Countering Challenges to the Global Supply Chain", [*accessed on 8 March 2014 at 0800 hrs]
[4] http://www.ic3.gov/ "*Internet Crime Report 2012*", [accessed on 11 March 2014 at 1300 hrs]

[5] B. B. Gupta, R. C. Joshi, Manoj Misra, ―ANN Based Scheme to Predict Number of Zombies involved in a DDoS Attack, International Journal of Network Security (IJNS), vol. 14, no. 1, pp. 36-45, 2012.

[6] Institute for Defense Studies and Analyses, *India's cyber security Challenge*, First Edition, March 2012

[7] http://hackmageddon.com/category/security/cyber-attacks-statistics/ *"2013 Cyber Attacks Statistics (Summary)*", accessed on 11 March 2014 at 0800 hrs]

[8] http://ncrb.nic.in/, "*Cyber Crimes*", [accessed on 11 March 2014 at 1400 hrs]

[9] http://en.wikipedia.org/wiki/National_Cyber_Security_Policy_2013, *"National Cyber Security Policy 2013*", [accessed on 11 March 2014 at 1000 hrs]

[10] http://www.indexoncensorship.org/2013/10/india-challenges-cyber-governance-cyber-security/, *"India challenges cyber governance and security"*, [accessed on 11 March 2014 at 0900 hrs]

[11] R. M. Johri Principal Director (information Systems) Office of CAG of India, "*Cyber Security – Indian Perspective"*

[12] ids.nic.in, *"Cyber Security in India's Counter Terrorism Strategy",* Col SS Raghav, [accessed on 10 March 2014 at 1300 hrs]

