DOI: https://doi.org/10.53555/nncse.v1i3.522 **Publication URL: http://nnpub.org/index.php/CSE/article/view/522**

CYBER SECURITY ISSUES AND RECOMMENDATIONS

Arushi Kohli[1]*, Akshya Raina[2]
*[1]Department of Information Technology Dronacharya College of Engineering
[2]Department of Information Technology Dronacharya College of Engineering

***Corresponding Author: -**

Abstract: -

Cyber Security is of real concern in today's period of figuring to secure information, system assets, and other discriminating data of an association. This paper presents prologue to digital security and the different dangers to the digital security and how these dangers can be determined. This paper additionally portrays the different difficulties of cyber security in India and Internet wrongdoing developing around the globe. Cyber security is currently not limited just to utilization of Internet on a Desktop PC yet securing data on Tablets, PDAs as they got to be paramount correspondence medium due to innovative progressions adult quickly in recent years. To determination issues identified with digital security the group of security scientists including the educated community, the private segment and government area must cooperate to comprehend the rising dangers to the figuring scene.

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

Because of absence of information security different digital criminal acts emerges, ―cyber security‖ means set of exercises, specialized and nonspecialized parts of ensuring information, gadgets, machine assets, system assets and other discriminating information put away there in from unapproved access, change and disturbance, revelation [1]. As indicated by rising digital danger report 2014 of Georgia Institute of Technology cell phones bring another set of dangers, including permitting malevolent programming an unparalleled research exploited person's lives. While ortable stages have to a great extent been ok for buyers and organizations, specialists and aggressors are discovering courses around the biological systems security [2]. Digital dangers are uneven on the grounds that assaults may be executed by the few upon a lot of people, with little cost and assets [3]. So digital security in Information engineering is of real concern in today's universe of figuring. As per Ic3[4] report 2012 (Internet Crime Complaint Center) a collusion between the National White Collar Crime Center (Nw3c) and Federal Bureau of Investigation (FBI) the main five nations by consider in exploited person objections numbered by Rank) as takes of

II. The Indian cyber space

The quick improvement of the Internet over the previous decade seemed to have encouraged an increment in the occurrences of Online assaults [5] In India National Informatics Centers were setup in year 1975 to give different IT related answers for the legislature. There were three significant systems were setup around then [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, for example, Defense, Energy, Finance, Space, Telecommunication, Transport and other open administrations intensely relies on upon the system to transfer information, for correspondence reason and for business transactions. So these divisions have a vast effect of utilizing the Internet as a wellspring of correspondence, and information as per National broadband arrangement the focus for broadband is 160 million family units by 2016 and the Networking list assesses that India's Internet movement will grow nine-fold in the middle of now and 2015. In spite of the fact that the legislature has aggressive plan to raise cyber integration, ecommerce administrations and correspondence channel yet in the meantime the administration ought to make solid approaches with respect to the cyber assaults and security. The legislature ought to make security against basic information framework through open private organization (PPP). Closed from the information drawn from worldwide details [7] the significant assault sorts are Hacktivism, cybercrime, cyber warfare and cyber espionage are shown in a chart demonstrating Attack Trends.

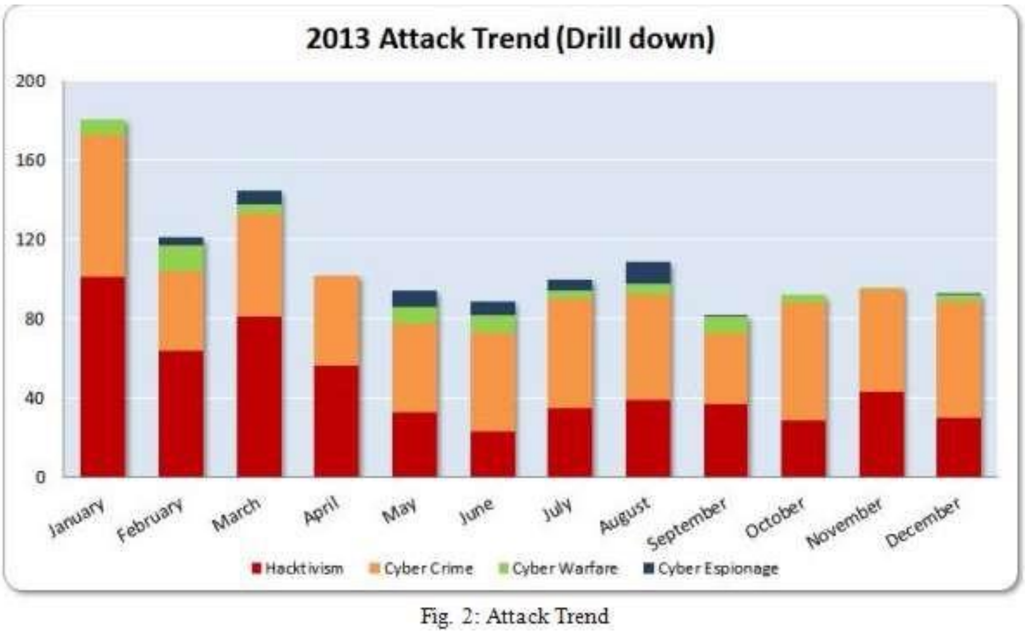
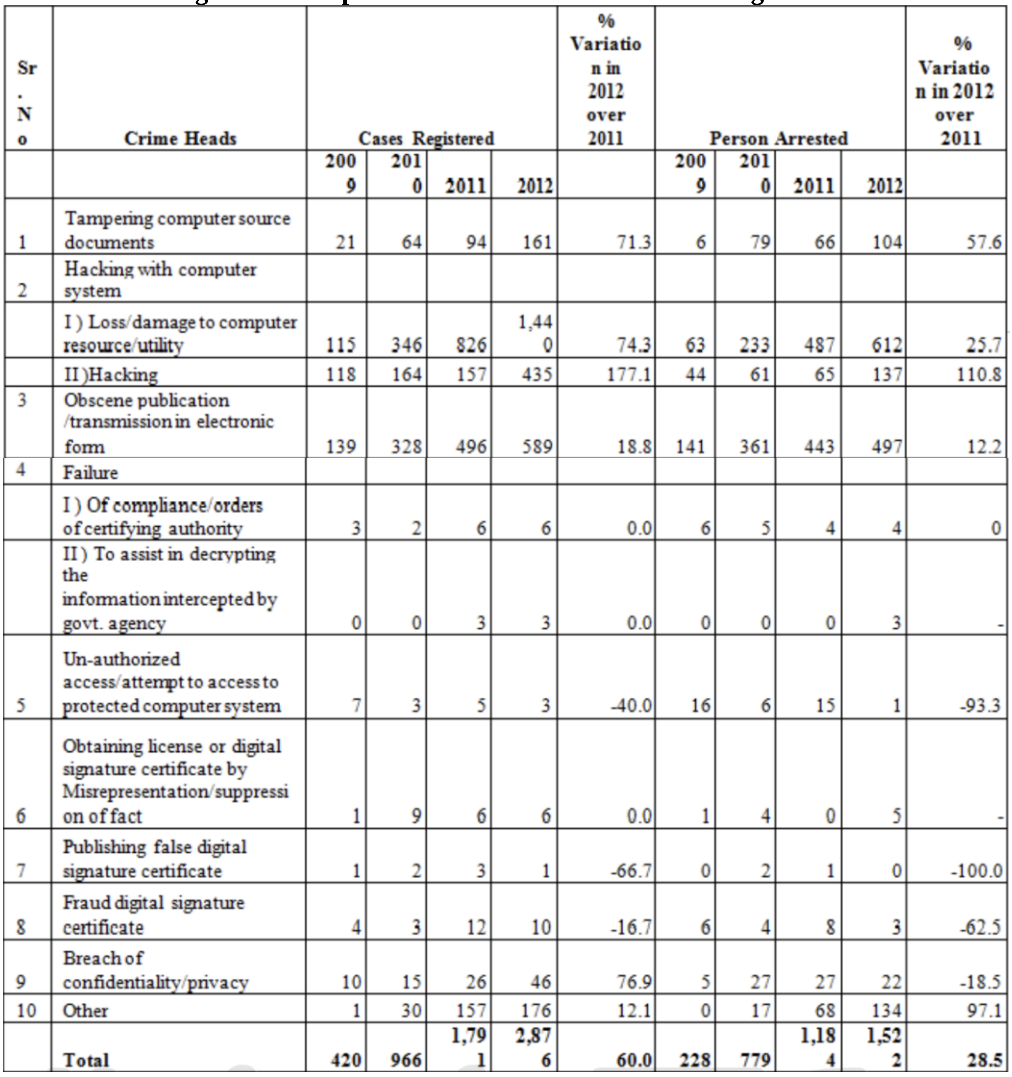


Fig. 2: Attack Trend

The following Table I shows Cybercrimes 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 Cybercrimes/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 strategy before 2013. In 2013, The Hindu, referring to archives spilled by NSA (National Security Agency) informant Edward Snowden, has affirmed that a significant part of the NSA observation was centered around India's residential governmental issues and its vital and business engages. This prompts flash chaos among individuals. Under weight, Government uncovered a National Cyber Security Policy 2013 on 2 July 2013 [9]. The Vision of the national security approach 2013 is to construct a safe and flexible cyberspace for residents, business and government. This approach is a proposed law by Department of Electronics and Information Technology, Government of India.

Which is, pointed towards ensuring general society and private base from cyber assaults. The approach additionally means to protect "data, for example, individual data (of web clients), money related and managing an account data and sovereign information". This was especially important in the wake of US National Security Agency (NSA) releases that proposed the US government organizations are spying on Indian clients, who have no lawful or specialized protections against it. Service of Communications and Information Technology (India) characterizes Cyber space is a complex environment comprising of collaborations between individuals, programming administrations underpinned by overall dispersion of data and correspondence engineering. Ministry of Communications and Information Technology (India) define following objectives of the sated policy

1. To make a safe cyber biological system in the nation, create satisfactory trust and trust in IT framework and exchanges in cyberspace and along these lines improve reception of IT in all divisions of the economy.
2. To make a confirmation structure for outline of security approaches and advancement and empowering activities for consistence to worldwide security norms and best practices by method for congruity appraisal (Product, process, engineering & individuals).
3. To enhance perceivability of uprightness of ICT items and administrations by making foundation for testing and approval of security of such item.
4. To give financial profit to organizations to appropriation of standard security practices and methodologies.
5. To empower Protection of data while in methodology, taking care of, capacity and travel to protect protection of subject's information and decreasing monetary misfortunes because of cyber wrongdoing or information robbery.

6. To empower compelling counteractive action, examination and arraignment of cybercrime and upgrade of low requirement abilities through proper authoritative mediation.

Days before the United Nation's headed Internet Governance Forum in Indonesia, India, held it – and first of its kind – meeting on cyber legislation and cyber security. With the backing of the National Security Council Secretariat of the Government of India, the two-day meeting was composed by private research organization Observer Research Foundation and industry body, Federation of Indian Chambers of Commerce and Industry, (FICCI). Speakers were from an assemblage of nations including Estonia, Germany, Belgium, Australia, Russia, Israel, and obviously, India. There are two expansive results of this gathering. The principal is that India has shown its eagerness to begin shouldering dialogs to do 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.

IV existing counter cyber security initiatives

Before researching the security activities to government territories that investment the be taken, take a gander at the chart [7] aggressors for interruption indicating different businesses and

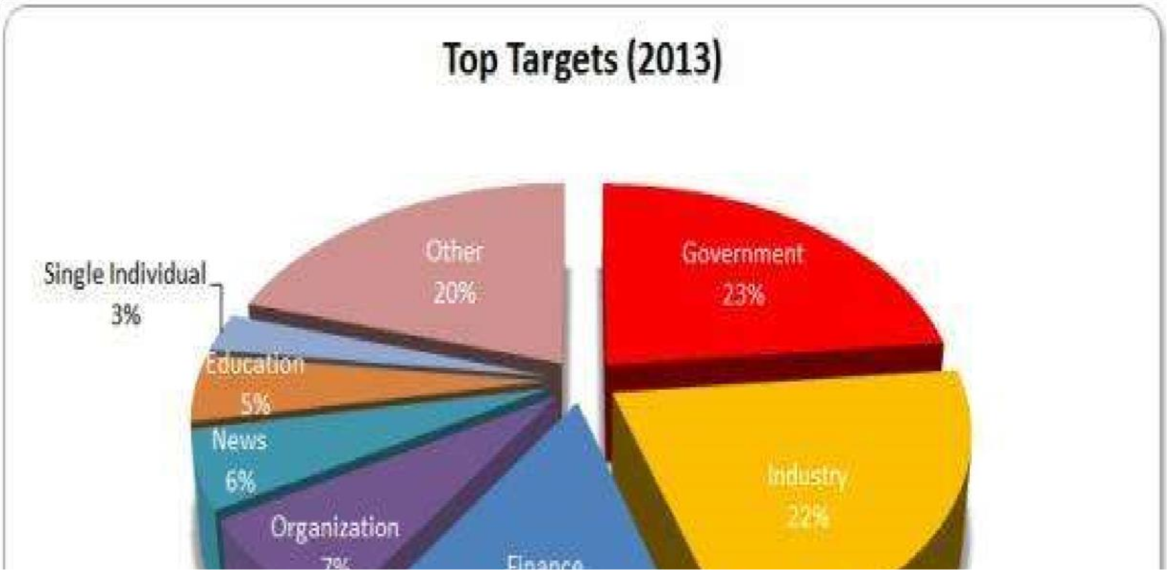


Fig.3: (Governments and Industries have been the most preferred targets for Cyber Attackers with similar values (respectively 23% and 22%). Targets belonging to finance rank at number three (7%), immediately ahead of News (6%) and Education (5%).)

So, on the proposals of ISTF [11] the accompanying activities have been taken:

1) Indian Computer Emergency Response Team (CERT-In) has been created to react to the cyber security episodes and make moves to anticipate repeat of the same.
2) Public Key Infrastructure (PKI) has been set up to help usage of Information Technology Act and advances utilization of Digital marks.
3) Government has been supporting R&d exercises through head Academic and Public Sector Institutions in the nation. A portion of alternate activities that can be taken [12]

A. National Informatics Center (NIC).

A head association giving system spine and e-legislation backing to the Central Government, State Governments, Union Territories, Districts and different Governments bodies. It gives extensive variety of data and correspondence innovation administrations including across the country correspondence Network for decentralized arranging change in government administrations and more extensive straightforwardness of national and neighbourhood governments.

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

Cert-In is the most vital constituent of India's cyber group. Its order states, 'guarantee security of cyber space in the nation by improving the security interchanges and data foundation, through proactive activity and compelling coordinated effort went for security episode counteractive action and reaction and security certification

C. National Information Security Assurance Program (NISAP).

This is for Government and discriminating foundations, Highlights are [12]:

(a) Government and discriminating foundations ought to have a security approach and make a state of contact.
(b) Mandatory for associations to actualize security control and report
(c) Cert-In to make a board of reviewer for IT security.
(d) All associations to be liable to an outsider review from this board once a year.
(e) Cert-In to be accounted for about security consistence on intermittent premise by the associations.

V RECOMMENDATIONS

A. Security Policy and Assurance

1) Critical division can be ensured by extemporizing the product advancement systems and framework building practices. So as to secure basic divisions more reinforced security models ought to be received.
2) Better preparation must be given with a specific end goal to help clients in IT security.

B. Early Detection and reaction

1) To stay away from noxious cyberspace exercises quick distinguishing proof and data trade techniques ought to be received.
2) Identification of key territories inside the basic framework.
3) Establish an open – private structural engineering for reacting to national- level cyber episodes.

C. Security preparing and Programs

1) National mindfulness projects, for example, National Information Security Assurance Program (NISAP) need to be advanced.
2) Providing preparation and training projects to help the Nation's cyber security needs.
3) Increasing the productivity of existing cyber security projects and enhancing space particular preparing projects, (for example, Law Enforcement, Judiciary, and E – Governance and so forth).

D. Promotions and Publicity

1) In India we have to compose different workshop projects, meetings, and examination programs in different IT foundations to upgrade cyber security aptitudes.
2) The advancement and attention crusade could incorporate courses, displays, challenges, radio and TV programs, features on particular themes, Web throws, Leaflets and notices, proposal and grant plans.

E. Specific Recommendations [6]:-

1) Emphasis ought to be set on creating and executing standards and best practices in government working and additionally in the private part. Cyber security reviews ought to be made mandatory for arranged associations. The standards ought to be implemented through a mix of regulation and motivating forces to industry.
2) The legislature ought to dispatch a National Mission in Cyber Forensics to encourage arraignment of cyber crooks and cyber terrorists.
3) The effect of the development of new informal communication media, and meeting of innovations on society including business, economy, national security ought to be considered with the assistance of applicable specialists, including political researchers, sociologists, anthropologists, clinicians, and law implementation masters. It ought to be guaranteed that the issues of security and human rights are not dismissed and a legitimate harmony between national security goals and human rights and protection is maintained.

VI CONCLUSION

In spite of the fact that the legislature has goaloriented arrangements to raise cyber network. There has a blast in e-business, and numerous exercises identified with e-influence are currently being completed over the Internet. As we become more subject to the Internet for our day by day life exercises, we additionally get to be more powerless against any interruptions brought about in and through cyberspace. The velocity with which this area has developed has implied that administrations and privately owned businesses are even now attempting to evaluate both the extension and significance of security in cyberspace and distributing obligation.

The cyberspace holds the fifth place in as something to be shared space and it is fundamental to have co appointments and collaboration among all countries with respect to cyberspace. The need of cyberspace and its abuse is becoming quickly. The cyberspace is getting to be vital range for huge number of terrorists to assault on critical data framework. The current laws are wasteful to control the cyber law violations and, along these lines urging a need to alter the current laws through which these exercises can be put on a check. There is a need of worldwide participation of countries to split down the effectiveness on cyber wrongdoing, consequently guaranteeing an improvement of the web cybercrime is not restricted to conditions of limits, accordingly it obliges a widespread cooperation of countries to cooperate to decrease the constantly developing dangers and danger to a sensible 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] http://www.ic3.gov/ ―*Internet Crime Report 2012*‖, [accessed on 11 March 2014 at 1300 hrs]

[4].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.

[5].Institute for Defense Studies and Analyses, *India's cyber security Challenge*, First Edition, March
[6].http://hackmageddon.com/category/security/cyber-attacks-statistics/ *" 2013 Cyber Attacks Statistics (Summary)*‖, accessed on 11 March 2014 at 0800 hrs]