International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 5 ǁ 2022 ǁ PP. 05-10

Best Practices for effective Cyber Security Execution in real world

Praveen Kumar S
PG Scholar, *Department of MCA, Dayananda Sagar College of Engineering, Bengaluru, Affiliated to VTU*

Mahendra Kumar
Assistant Professor, Department of MCA, Dayananda Sagar College of Engineering, Bengaluru, Affiliated to VTU

Abstract— *In the arena of computer age cyber security is a big concern to prevent resources of networks, confidential data and crucial information in an organization. The motive of this paper is to highlight the different types of cyber threats and their solution to overcome from them. Besides that, it also describes the different aspects of cyber crime and its security in the global world. Now-a-days, with the expansion of internet usage, cyber security is not restricted to a personal workstation, but also used to suppress information of personal mobile devices like tabs and cell phones because they have become very imperative medium of information transfer due to the current advancements in technology. In order to resolve cyber security issues, the security researcher's community including government sector, academia, private sector must work together to understand the emerging threats to the computing world.*

Keywords—*NIC (National Informatics Centre), Cyber Crime, Cyber Security, NISAP (National Information of security Assurance Program), ISTF (Inter Departmental Information Security Task Force), IC3 (Internet Crime Complaint Centre),*

Date of Submission: 12-05-2022 Date of acceptance: 26-05-2022

I. INTRODUCTION

Fast developments in technology provide recent scope of efficiency for organizations that leads to the introduction of significant threats to the information and data of organizations. Cyber security states the protection of systems, data and networks in cyber world which is a captious affair for all business organizations. Cyber safety will be very crucial as the number of devices connected to the internet will increase, which will be at a rapid pace. Cyber threats can be categorized as below:

- *Cyber terror*

An independent working organization, that conducts activities that leads to terror using cyberspace medium for spreading the same.

- *Cyber crime*

Any activity that intends for the extraction or theft of confidential data, money or unethical hacking, Examples of cyber crime can be crashing down a service or website or acquisition of intellectual property and credit/debit card data.

- *Cyber war*

An attempt to damage the computers or information networks of a nation or international organization by another state- nation or organization by any means like dos attacks or computer viruses.

Cyber threats are mainly asymmetric since these are committed by most with least resources and cost. Due to this, cyber crime is big threat in the present scenario of the Internetworking. As per the Internet Crime Complaint Centre report 2015, the top countries having most victim complaints (in numbers) are as below.

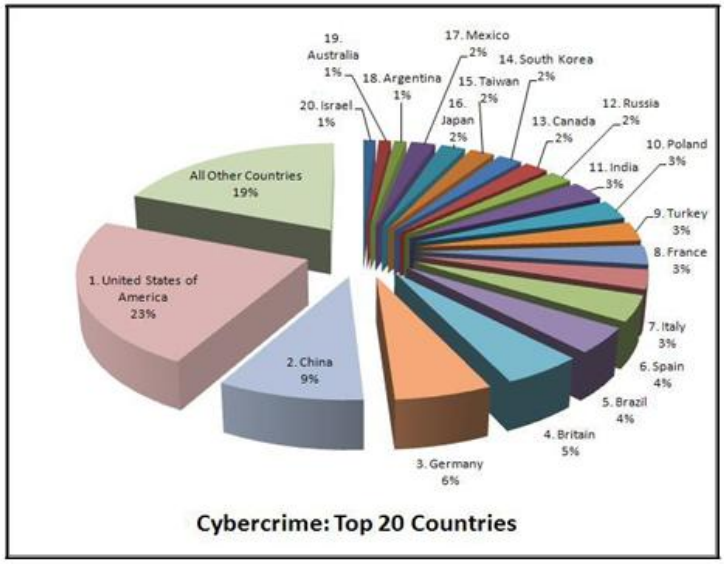

Fig. 1- Top 20 Countries by count: Cyber Crime Complaints

II. CYBER SPACE OF INDIA

There is an increase in the online cyber attacks incidents with the speedy development of Internet usage in the last decade. NI C's in India were established in the year 1975 in order to provide solutions related to IT to government. Main networks that were setup at that time were:

(a) INDONET: - To connect IBM mainframes servers which made up computer infrastructure of India.

(b) NIC NET: Inter network used in public organizations to connect Centre with the state, and other administrations at district level.

(c) ERNET: - ERNET stands for Education Research Network and is used to serve the purpose of academics and research communities.

Defense, Finance, Energy, Space, Transport, Telecommunication and other public services are critical sectors that majorly dependent on computer networks to broadcast data, for communication as well as commercial purpose. So, there is a huge impact of using Internet in these fields as source of information and communication as per NBS. 170 million broadband connectivity will be provided to the households by 2017, this is a per the target mentioned by Networking Index, between 2014 to 2019, Internet traffic will reach up to 4.2 folds. An aspiring scheme to increase the internet connection has released by Indian Government, communication channel and E-marketing but government should make strong security policies for cyber crime and unethical cyber attacks. The government should go for public private partnership (PPP) in order to make protection against critical information infrastructure. The data drawn from global statistics of the year 2015 indicates, the major types of cyber attacks are cyber crime, Hacktivism, cyber espionage and cyber warfare. Same is displayed in a graph.

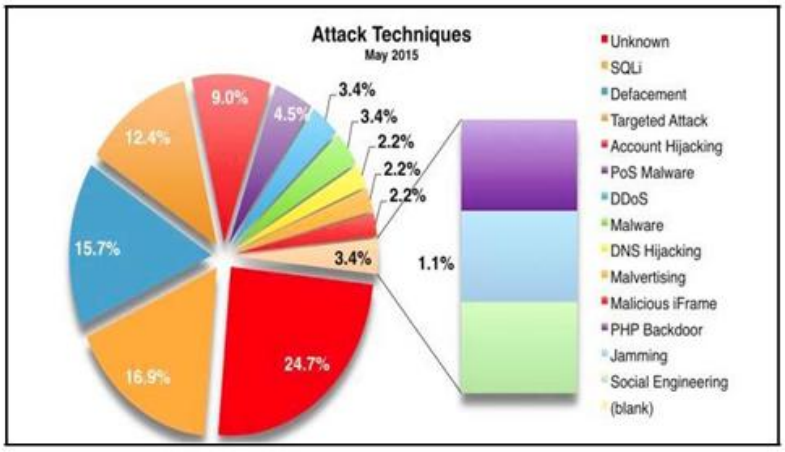

Fig. 2 -Attack Trends of India in the year 2015

Table1: Cyber Crime cases reported & resolved by IT Act

S. No.	Types of Cyber Crime	Reported cases				Percentage Deviation in 2014-2013	Action taken by prosecution				Percentage Deviation in 2014-2013
		2011	2012	2013	2014		2011	2012	2013	2014	
1	Manipulating confidential documents	25	68	120	180	50	10	90	70	120	71
2	Computer Hacking										
	*System Hacking	120	180	210	520	147	64	71	75	160	113
	*Damaging of Resources	130	380	850	1460	71	73	266	520	640	23
3	Disruption in E- data transfer	150	348	525	614	16.9	161	392	485	532	9
4	Access of system by un-authorized user	12	8	10	7	-30	21	9	20	4	-80
5	Allow Fake certificates of Digital signature	4	6	7	2	-71	2	4	3	2	-33
6	Digital Signature scam	8	5	15	12	-20	8	5	9	4	-55
7	Security Breach in private information	15	20	31	52	67	10	32	32	31	-3
8	other	3	40	180	197	9	2	22	73	150	105
	Total	612	1055	1948	3344	243	353	887	780	970	212

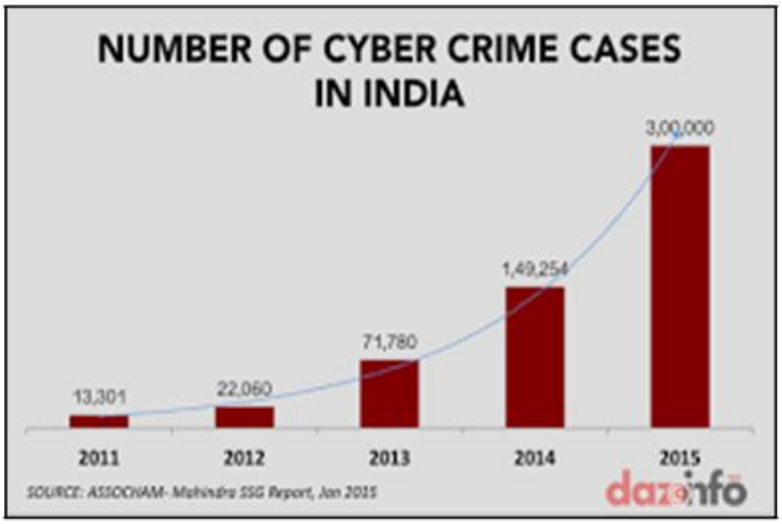

Fig. 3- Cyber Crime Annual Graph.

III. NATIONAL CYBER SECURITY POLICY 2013

In 2013, India launched their Cyber policies to stop cyber crime and cyber attacks. As per "The Hindu" in 2013, NSA (National Security Agency) whistleblower Edward Snowden alleged that much of the NSA surveillance was focused on domestic politics of India
& its strategic and commercial interests that leads to spark rage among Indian people. Under tremendous pressure, government of India brought a National Cyber Security Policy 2013.

Vision: *To build a secure and resilient cyberspace for citizens, business and* government. [1]

Mission: *To protect Information and Information cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of Institutional structures, people, processes, technology and cooperation. [1]*

Department of Electronics and Information Technology, India proposed a law for Cyber Security which is known as National Cyber Security policy and is aimed for prevention from cyber attacks of private and public infrastructure. It also speculates safe information like financial and banking information, sovereign data and personal information of users which was somewhat relevant of US NSA(National Security Agency) leaks that indicates spying on Indian users by US government, who have no technical or legal safeguards for it.

OBJECTIVE:

Ministry of Communications and Information Technology (India) defines Cyber space is a wide and complex environment consisting of communication 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.

Private think-tank Observer Research Foundation & Industry body, FICCI conducted a conference with the collaboration of NSCS by the Government of India. There were many speakers presented the conference including the host of the countries like India, Belgium, Russia, Australia, Estonia, Germany, Russia. The two major outputs have come after this conference: firstly, India has shown its eagerness to initiate cyberspace open discussions globally. And secondly, India has made a NATIONAL CYBER SECURITY POLICY rather than strategy of cyber security; this was stated by National Security Advisor of India. The outcome of this Conference made a distribution of targets to the various sectors in India as shown in fig. 4

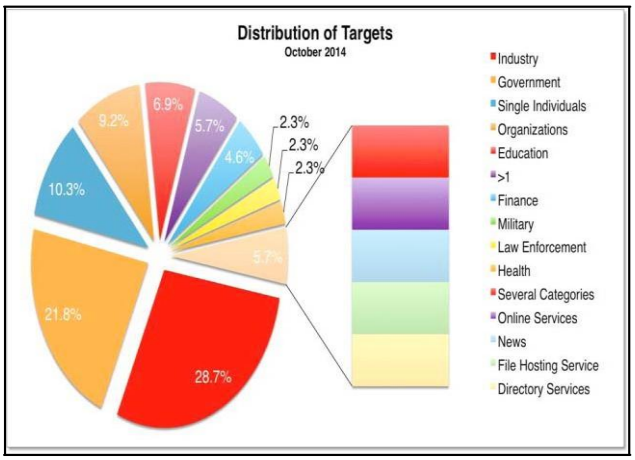

Fig. 4: Distribution of Targets

Some Initiatives taken by Indian Government for Cyber Security:

Recommendations of The Internet Science and Technology Fair, some steps taken by Indian Government:

1) A team has been established named, "Indian Computer Emergency Response Team" to rectify the problems relevant to the cyber crime and attacks and capable to take decisions to stop this kind of activities.
2) To Encourage exertion of Information Technology act PKI (Public Key Infrastructure) has been established and usage of Digital Signature can be promoted.

3) In the Country, prime Academic Institutes and Public Sector Organizations will enhance research and development with the help of Indian Government.

IV. FEW STEPS TAKEN BY INDIAN GOVERNMENT FOR CYBER SECURITY

A. Cert-In:-Indian Computer Emergency Response Team

Cyber community of India has a vital constituent: (Cert- In). Policy of this team assures that they enhance the information infrastructure and security of confidential cyber safety of global cyber world in India by their adequate collaboration and proactive action aiming to prevention of security incidents

B. National Informatics Centre (NIC).

National Informatics Centre was the first organization which provides e-governance and backbone networking to assist Union Territories, State Government & Central Government and other existing Government Bodies. Wide range of Communication and information technology including improved decentralized scheme for global communication network was provided by NIC to huge clarity in Local and National Government issues.

C. National Information Security Assurance Program (NISAP).

The NISAP was made up for crucial infrastructure and for Government Issues:

(a) There should be a firm security policy and direct point of contact in case of emergency for crucial infrastructure and Government.

(b) Security control policy is compulsory to implement in any organization and to report CERT-IN team immediately after any disrupted incident.

(c) An auditor panel has to be made for IT security by CERT-IN.

(d) All the organizations are forced to report on regular basis about the compliance to CERT-IN

V. RECOMMENDATIONS

A. Assurance and Security Policy

1) By contriving new software development technologies & practices of system engineering crucial sectors can be protected. There is an urge to build more liable model for cyber security to prevent crucial sectors.

2) Good knowledge and training should be given to IT security to support them.

B. Response and early sensing of malicious program

1) Some effective data & information exchange and speedy identification ways must be followed up to stop the malicious activities in cyber world.

2) In the captious infrastructure some immediate identification of key areas should be adopted.

3) For the proper handling of national level cyber crime activities government should set up private and public infrastructure.

C. Programs and security exercise

1) Government should conduct proper workshops and knowledge sessions to groom the needs of cyber security globally.

2) There is a need to enhance the ratio of current cyber security sessions and to provide the training workshops n specific domain. Like Judiciary, Law Enforcement & E-governance etc.

3) Workshops for global awareness like NISAP (National Information Security Assurance Program) must be conducted.

D. Aggrandizement and Promotion

1) There is an urge to boost the cyber security skills in Different IT organizations by conducting conferences, research workshops, training sessions and seminars.

2) The promotion of cyber security knowledge could include radio publicity and TV ads, webinars, online contests, promotional links on social media, newspapers, banners, posters, conference, videos on relevant topics on periodic basis.

E. Explicit Suggestions:-

1) Implementation and development should be prioritized & proper sessions should be given in government community as in private sector. All networking organizations are compulsory for periodic cyber audits.

2) To expedite the prosecution of cyber terrorists and cyber criminals National Mission of Cyber forensics has to be launched by Government of India.
3) It must be assured that the concern of human rights and its privacy are invisible of imperatives global cyber security & also privacy and human rights must be conserved.

VI. CONCLUSION

In present scenario there is a sudden rise in E- business & E-marketing and other endeavors relevant to electronic-commerce and E-governance. Our daily life routine activities are also getting more dependent on internet, beside that we also getting more susceptible to get caught in any mishap through cyber connectivity. Government and private companies are still finding out the ways to resolve both cyber crime in cyberspace and accounting responsibility. The cyberspace stands fourth in common space and it is important for all of us to have co-ordination and cooperation among all countries of the world for security of cyberspace. As there is a big rise in need of cyberspace, its exploitation is increasing on a very rapid pace. Now-a-days, cyber security is becoming very important and crucial area for lager number of terrorist attack on important and critical information centre. Present laws are not efficient enough for preventing the cyber threats and there is a great urge for rectification of these laws and needs to be check timely and modify according to the betterment of Indian Society. International cooperation is the need of hour to crack down an efficient law to handle cyber crime which is not confined to boundaries of states and thus an universal collaboration of states is required to plan together in order to reduce the rapidly increasing cyber crime & cyber risk to the least level.

REFERENCES:

[1]. http://deity.gov.in/sites/upload_files/dit/files/Nationa l%20Cyber%20Security%20Policy%20%281%29.pdf accessed on 18 jan2016 at 1100 hrs.
[2]. Douglas A. Barnes. Deworming the internet. Texas Law Review,83:279–329, November 2004.
[3]. Seymour E. Goodman and Herbert S. Lin, editors. Toward a Saferand More Secure Cyberspace. National Academies Press, 2007.
[4]. United States Department of Justice, editor. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. 2002.
[5]. Paul Ohm, Douglas Sicker, and Dirk Grunwald. Legal Issues Surrounding Monitoring (Invited Paper). In Internet Measurement Conference, October 2007.
[6]. Yang and J. Lui. Security adoption in heterogenous networks: The influence of cyber-insurance market. In IFIP Networking , 2012
[7]. M. Lelarge and J. Bolot. Economic incentives to increase security in the internet: The case for insurance. In IEEE INFOCOM , 2009
[8]. A. Khouzani, S. Sen, and N. Shroff. An economic analysis of regulatingsecurity investments in the internet. In IEEE INFOCOM , 2013
[9]. Cui Jing, Liu Guangzhong, the basics of computer network [J]. Tsinghua University Press,2010.07.01. [10]Daniel J. Solove. Digital dossiers and the dissipation of fourth amendment privacy. Southern California Law Review, pages 1083–1167, 2002.