IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-5, Issue-12 E-ISSN: 2347-2693

Cyber Security Policies for Digital India: Challenges and Opportunities

Singh Anurag[1*] and Singh Brijmohan[2]

[1*]Department of Computer Application, COER School of Management, Roorkee, India
[2]Department of Information Technology, COER, Roorkee, Uttrakhand, India

[*]*Corresponding Author: anuragmaddi@gmail.com*

Available online at: www.ijcseonline.org

Received: 11/Nov/2017, Revised: 23/Nov/2017, Accepted: 12/Dec/2017, Published: 31/Dec/2017

Abstract- India is perched on the cusp of computerized development. The administration has defeated its depreciators with a hawk looked at center to accomplish this objective for the nation. It is currently up to organizations to guarantee they are prepared and arranged to load and attempt the open doors this advancement will bring. The Indian government has lodged on a program to transform the nation into an advanced economy. It has make open a progression of activities—from presenting Digital Locker, which takes out the requirement for individuals to convey printed versions of reports issued by the administration, to demonetization, which has impelled the utilization of computerized installments the nation over. The move towards an advanced economy is probably going to help enact a new rush of financial development, draw in greater venture, and make new employments, over numerous divisions. Notwithstanding, it additionally represents a major test, that of cybersecurity. With the move towards a computerized economy, expanding measure of buyer and national information will be put away carefully and an extensive number of exchanges will be done on the web, by organizations, people and also government divisions. In any case, it additionally represents a major test, that of cybersecurity. With the move towards a computerized economy, expanding measure of shopper and national information will be put away carefully and a substantial number of exchanges will be completed on the web, by organizations, people and also government divisions. That makes India a greater focus for digital lawbreakers and programmers. Different partners, particularly Indian organizations, should be better arranged to deal with this risk. National cybersecurity technique is a fundamental component as cybersecurity is expected to ensure also, empower computerized economy.

Keywords -cybersecurity, Digital India, Online transaction, personal data security, national cybersecurity strategy, cyber threats, cybercrime.

I. INTRODUCTION

The cost of cyberattacks in India as of now remains in overabundance of Rs25,000 crores ($4billion). It is imperative to take note of that there are numerous cyberattacks that go undetected and unreported too, so this number could be substantially higher. The misfortunes radiate from operational interruptions, loss of touchy data and plans, client stir and effect on mark picture, and also increment in lawful cases and protection premium. The issue is estimate to expand facilitate in the coming years, coming to as high as Rs1.25 trillion ($20 billion) throughout the following 10 years, as the business operations of most Indian organizations move toward becoming arranged. Thus, organizations in India should be proactive to guarantee they cultivate effectiveness and viability in cybersecurity administration. The vision for this needs to originate from the extremely top. It is essential that the CEOs make this a high need on the administration plan and fabricate plainly characterized security guides to have a more organized execution in accordance with their security technique.

II. WHY INDIA NEED IT

The most recent report discloses to us that India had 4,621.24989 Internet supporters in September 2016. In light of a populace tally of 127.7 crore, it makes an interpretation of this into 28.77 Internet supporters for every 100 populaces. The general IP traffic is required to grow four-overlap from 2016 to 2021, a compound annual development rate (CAGR) of 30 for every penny and achieve 6.5 Exabyte of information for each month in 2021, up from 1.7 Exabyte for every month in 2016, Cisco estimates. 67% recognized no less than one cybercrime. Nearly 60% distinguished at least one writes of digital assault. 11% recognized digital theft.24% identified other PC security incidents. Most organizations did not report digital assaults to law implementation authorities. The greater part of deceived organizations (86%) distinguished numerous

occurrences, with half of these (43%) identifying at least 10 episodes amid the year. Approximately 68% of the casualties of digital robbery maintained money related loss of $10,000 or more. By correlation, 34% of the organizations identifying digital assaults and 31% of organizations distinguishing other PC security occurrences lost more than $10,000. Framework downtime endured in the vicinity of 1 and 24 hours for half of the organizations and over 24 hours for 33% of organizations distinguishing digital assaults or other PC security episodes (https://www.bjs.gov/).Of the 11,592 instances of cybercrime revealed in 2015, upwards of 8,045 were documented under the Information Technology (IT) Act, while 3,422 were recorded under the Indian Penal Code and 125 under exceptional and nearby laws. Upwards of 8,121 individuals were captured in 2015 for cybercrimes, a 41 for each penny increment from 2014. Around 36,000 cases were enlisted in the vicinity of 2006 and 2015, while 24,140 people were captured. The people captured for professedly carrying out digital violations expanded 14 times over the previous decade, demonstrating this speaks to an expanding issue, as India moves towards more noteworthy digitization. There was a 13 for each penny increment in India's web supporter construct, from 302.4 million with respect to March 31, 2015, to 342.7 million on March 31, 2016, as indicated by information tabled in the Lok Sabha. The Global Cybersecurity Index (GCI) is a multi-partner activity to quantify the dedication of nations to cybersecurity. Cybersecurity has a wide field of use that cuts crosswise over numerous businesses and divisions. Every nation's level of improvement will in this way be dissected inside five classes: Legal Measures, Technical Measures, Organizational Measures, Capacity Building and Cooperation.

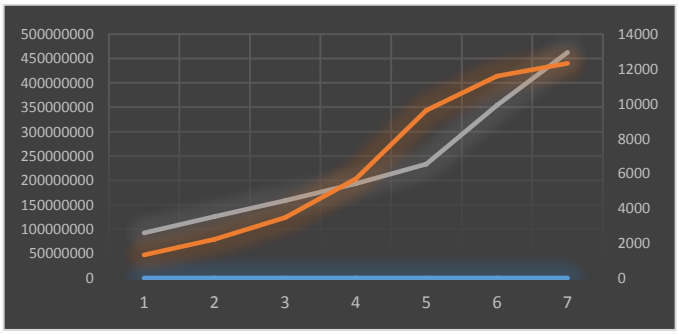

Fig. 1 Growth rate Of Internet Users and the Cyber Crime (India)

Table 1

Year	No. of Cyber Crime Cases	Internet Users (in lacs)
2010	1322	923.23838
2011	2213	1,256.17813
2012	3477	1,589.60346
2013	5693	1,932.04330
2014	9622	2,331.52478
2015	11592	3,541.14747
2016	12317	4,621.24989

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.973[a]	.947	.937	1885.81829

a. Predictors: (Constant), Interne User

Table 2

Coefficients

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	-4630.069	1520.451		-3.045	.029
	Interne_User	5.501	.581	.973	9.476	.000

a. Dependent Variable: Crime

Linear equation

Number of Cyber Crime= -4630.069+ 5.501(Number of Internet Users in Lacs)

As shown in figures and tables that as number of internet users are increasing year by year and in the same way number of cybercrime cases are also increasing. India is moving towards Digital India so internet users will increase so India need some planning or strategy to handle the situation. Otherwise situation will be out of the control.

III. INITIATIVE TAKEN TO HANDLE CYBERCRIME PREVENTION IN INDIA

a) Crime and Criminal Tracking Network and Systems (CCTNS)

Affirmed by the Cabinet Committee on Economic Affairs in 2009, with an assignment of INR 2 billion, the CCTNS is a task under the National e-Governance Plan. It goes for making an across the nation organizing foundation for an IT-empowered criminal following and wrongdoing location framework. The mix of around 15,000 police headquarters, locale and state police home office and robotized administrations was initially planned to be finished by 2012. Notwithstanding, this still stays fragmented. Aside from the moderate pace of usage and budgetary issues, on-the-ground obstacles to completely operationalizing CCTNS incorporate problematic Internet availability and under-prepared work force at police headquarters. Different issues incorporate inaccessibility of offices for digital measurable investigation in many areas, and absence of mindfulness seeing on the web

nationals' administrations, for example, check of occupants and representatives and freedom for parades and occasions.

b) Online Complaints

The Central Government, in light of questions by the Supreme Court with respect to measures taken to handle cybercrime, as of late declared that they would set up an 'Inside Citizen Portal'. This entrance will enable residents to document grievances online regarding cybercrimes, including digital stalking, online money related extortion and others, endured or saw by them. The legislative reaction likewise points of interest the proposed procedure, expressing that any such dissension on the entrance will trigger an alarm at the applicable police headquarters and enable the police division to track and refresh its status, while the complainant too would have the capacity to see refreshes and raise the grievance to higher authorities.

c) Cyber Police Stations

Digital police headquarters for the most part incorporate prepared work force and also the proper gear to examine and track advanced wrongdoings. Maharashtra, where cybercrime has ascended more than 140% as of late, and which had the troubling refinement of just chronicle a solitary conviction identified with cybercrime a year ago, is changing over its current cybercrime labs into digital police headquarters. This will mean there is a digital police headquarters in each region of the state. The activity in Maharashtra is valuable particularly as a result of the ascent in online exchanges in Tier II and Tier III urban areas and the rising cybercrime related thereto. In any case, regardless of the ascent in cybercrime, grievances stay of low reportage and low achievement rates in understanding wrongdoing. Cops point to issues handling proof, with complex methodology being required to recover information on servers put away abroad. Further, there have been protestations in Bengaluru of the constrained purview of digital police headquarters. As per a standing request of the DG and IGP of Bengaluru City Police issued in June 2016, just cases with harms of over INR 5 lakh can be enrolled at digital police headquarters if there should arise an occurrence of bank card extortion. In instances of web based bamboozling, just those cases where harms surpass INR 50 lakh are agreeable to the purview of digital police headquarters. Every single other case are to be enlisted with the neighborhood police headquarters which, not at all like digital police headquarters, don't for the most part incorporate prepared work force or the proper hardware to examine and track advanced violations.

d) Predictive Policing

Prescient policing includes the use of information mining, measurable demonstrating and machine learning on datasets identifying with wrongdoings to make expectations about likely areas for police mediation. Cases of prescient policing incorporate problem area mapping to distinguish worldly and spatial hotspots of criminal movement and relapse models in view of relationships between prior, generally minor, wrongdoings and later, rough offenses. In 2013, the Jharkhand Police, in a joint effort with the National Informatics Center, started building up an information digging programming for checking on the web records to examine wrongdoing patterns. The Jharkhand Police has additionally been investigating business examination aptitudes and assets at IIM-Ranchi, so as to handle wrongdoing in Jharkhand. The Delhi Police has taken advantage of the aptitude at the Indian Space Research Organization with a specific end goal to build up a prescient policing instrument called CMAPS – Crime Mapping, Analytics and Predictive System. The framework distinguishes wrongdoing hotspots by joining Delhi Police's Dial 100 helpline calls information with ISRO's satellite symbolism and picturing it as bunch maps. Utilizing CMAPS, Delhi Police has cut its examination time from the 15 days it brought with its past mechanical wrongdoing mapping to the three minutes it takes for the framework to invigorate its database. The Hyderabad City Police is building a database, called the 'Incorporated People Information Hub' which, as indicated by the City Police Commissioner, would offer the police a "360-degree see" of residents, including names, assumed names, family subtle elements, locations and data on different reports including travel papers, Aadhaar cards and driving licenses. The information is brushed from a boundless assortment of sources, including data on captured people, guilty parties' rundown, FIRs, telephone and power associations, expense forms, RTA enlistments and e-challans. It is additionally recorded with remarkable identifiers, and is utilized to build up the genuine character of a man, and present outcomes to pertinent specialists inside minutes. While the framework is gone for controlling criminal movement and recognizing extortion, an absence of obviously distinguished digital security and protection conventions is a stressing sign.

IV. STEPS TO PREVENT CYBER CRIME

a) Establish a National Cybersecurity Strategies

As nations capitalizing on digital revolution, cybersecurity is a national priority to foster economic welfare. Based on NATO and ENISA, in the period of 2013-2016, there is a total of 48 national cybersecurity strategies (NCSS) released.

In NCSS, the main objectives are maintaining secure, resilient and trusted electronic operating environment, promoting economic and social prosperity, promoting trust, business and economic growth, addressing risk of ICT and strengthening resilience of infrastructures. India do not have any NCSS policy.

b) Adjust national priorities

To set a decent illustration, the United States and different nations should make the battle against cybercrime a need, as a general rule and not simply openly articulations. More assets must be carried out to distinguishing, catching, and indicting digital culprits, whoever they are and wherever they are found. Expanding federal law enforcement authority to deter the sale of spyware used to stalk or commit ID theft. Giving courts the authority to shut down botnets engaged in distributed denial of service attacks and other criminal activity. Updating the Racketeering Influenced and Corrupt Organizations Act (RICO) so that it applies to cybercrimes. Clarifying the penalties for computer crimes. Making sure these penalties are in line with other similar non-cybercrimes.

c) Catch more criminal's faster

It may strike you as blindingly evident that we have to get more cybercrime culprits speedier, however there is a reason I have gotten this out. The scope of measures accessible to deflect offenders incorporates expanding sentences for those indicted, expanding the likelihood of being indicted, and expanding the speed with which criminal acts are rebuffed. In the scholarly investigation of wrongdoing, known as Criminology, there has been a great deal of research into which of these measures are best in discouraging criminal movement. At the end of the day, while it may regard ensure that digital violations convey sentences which mirror the immense mischief they incur on individuals and society, stiffer sentences alone won't do much to discourage hoodlums unless we get a greater amount of them speedier. What's more, that requires better utilization of current assets, as well as, as I would like to think, extra assets committed to getting digital offenders.

d) Measure the Problem

Reliable endeavors to unbiasedly gauge the issue of cybercrime are eminent by their nonattendance or insufficiency in the English-talking world. Putting forth the defense for more assets to battle cybercrime requires strong proof of the scale and extent of the issue.

e) Enhancement required in Cyber Appellate Tribunal

India requires a multiple Cyber Appellate court. Currently India has only one Cyber court in and that is also not functioning properly. There are so many cases are in pending state. On the other hand, China launched its first cyber court focusing in conduct Internet-related cases in the e-commerce hub of Hangzhou amid a spike in the number of online disagreements. So India need to improve its Cyber Appellate Tribunal infrastructure as well to handle a Cyber Crime cases.

V. CONCLUSION AND FUTURE SCOPE

In advanced economy, development is changeless. The Digital Upheaval balanced new difficulties to business and countries, as limits are tried and re-imagined always. Advanced economy use on the internet and it is combined with the advancing digital dangers. For countries to thrive in advanced economy, availability in innovation condition and organized framework relies upon the trust and certainty of the partners, in particular government, private area and people. These trust and certainty of the partners are the empowering agent of the computerized economy. One of the techniques to expand trust and trust in the internet is execution of national digital security techniques which address cybersecurity issues. The normal accentuation of the NCSS broke down are basic framework assurance, cybercrime security, cybersecurity proficient advancement, cybersecurity open mindfulness, innovative work (Research and development) and universal joint efforts. In this exploration, the availability of country to procure advanced economy isn't connected to the improvement and production of the country's NCSS. All together for computerized economy to flourish, the advanced certainty of the partners is high. Countries with high computerized certainty like Singapore, depend less on the national level NCSS to fortify the trust and trust in computerized space. The NCSS is as yet a need to concrete the cybersecurity of the country, as cyber threats and dangers continue developing. Singapore is starting to heighten its endeavors and duty in national cybersecurity. The other best ten countries in advanced economy existing has a NCSS. It gives the essential establishment to computerized economy to thrive further. A NCSS isn't a prerequisite for country to start advanced economy, nonetheless, NCSS is a necessity for a country to constantly create and be effective in advanced economy.

VI. METHODOLOGY

This article in view of writing research. The scientist got to data from assortment of literary works, in light of diary articles, worldwide reports, current industry happenings and market patterns. After the literary works are accumulated, the analyst sorts them out to decide the pertinence to settle the delegate writing to the point. The pertinence of the literary works picked depend deliberately, expert, adequacy and dependability With the end goal of the examination, the agent literary works picked were from year 2010 - 2017. The issues in cybersecurity are present and quick moving. Delegate writing on the theme should be present to be significant. In this examination, reports, diary article and innovation news from dependable sources were incorporated.

VII. REFERENCES

[1] (October 2017) www.securingourecity.org
[2] (October 2017) www.ccdcoe.org
[3] (October 2017) www.smeru.or.id
[4] (2010 October-December 2017) ncrb.nic.in
[5] (2010 September-October 2017) www.internetlivestats.com
[6] (October 2017) http://www.business-standard.com/

