CYBER CRIME AND MEDIA AWARENESS IN INDIA (QUANTITATIVE ANALYSIS METHOD)

Ravichandran Kamalakannan
Department of Media Sciences, Anna University, Chennai-600025 Tamil Nadu, India
ravi.news10@yahoo.com

ABSTRACT

Computer and cellular phone based crimes have elevated alarmingly in India. From the unauthorized dissemination, preserving statistics systems secure from tampering and from unauthorized removals are the want of the hour, otherwise, the incidents of hacking, facts theft, cyber bullying and now cyber extortion as nicely has kept the cyber safety team on its feet. For this, a majority of the respondents represents that is 60 percent felt that most effective on occasion the media is giving cyber crime related information. 25% in keeping with cent stated they did not find enough news associated with cyber protection, even as handiest according to 20% had been of the opinion that cyber crime associated information seem in media very often. Of the last 20%, 5% were of the opinion that print media is creating more awareness and 80% stated, it is far the digital media that is growing people more privy to on troubles associated with cyber crime. Quantitative evaluation in the fashion of a survey became instrumental in gathering the statistics that has analyzed by the ANOVA test; Multivariate Tests, Normative evaluation, Structural Equation Model, and Model match assessment. Along with this, measures has analyzed to control cyber crime also have also been mentioned.

INTRODUCTION

India is one of the populous countries and booms in crime rate is a reason for worry for the Indian economic system and to the Indian government at massive. Particularly PC based cyber crimes are also growing and there is a more threat to the kingdom. Computers play a very giant function in modern life. A Number of people who has to get entry to information on the computers and the maximum of the industrial and government records and unrestricted access to records gift an actual chance (Janna Anderson,2014), (Ben Brandt,2011). From the unauthorized dissemination, keeping data systems relaxed from tampering and from unauthorized removals are the want of the hour, otherwise, the incidents of hacking, statistics robbery, cyber bullying and now cyber extortion as properly has kept the cyber protection crew on its ft (National Crime Records Bureau Ministry of Home Affairs,2015). Significantly, Website builders, the Internet, and networking software program professionals are hardly ever able to manipulate this risk. Such violations can also debilitate a rustic's protection and money associated well-being troubles encompassing these forms of crimes have turned out to be prominent, especially the ones encompassing hacking, copyright encroachment, tyke erotic amusement, and child making ready (Internet security Threat Report 2014)..

LITERATURE REVIEW

The records at the boom in cyber crime in India are alarming. Consistent with the January 2015 document of the associated Chambers of Commerce and industry of India, the quantitative of cyber crimes in India would have touched a decade of 3, 00,000 ultimate twelve months. Hacking, expertise robbery, cyber bullying and even cyber extortion had been on a constant rise. Mumbai Police is celebrating 'Cyber protection Week' and utilizing its authentic Twitter take care of along with that of the Commissioner of Police to proportion public service messages — with memes and quirky one-liners to help unfold recognition on cyber crime (Vinit Kumar, Sharda Avdhanam,2013). They have been given, even used the lately long gone viral 'Be like invoice' meme to attach with their audience and consider it, their messages are spot on. With growing web penetration, cyber crimes have also increased in the final few years. Between 2011 and 2015, a number of cyber crimes registered inside the country have lengthy beyond up 5 events.

Maharashtra & Uttar Pradesh has accounted for one-third of these crimes. With growing cellular and net penetration in United States of America, cyber crimes have additionally prolonged proportionately. Between 2011 and 2015, greater than 32000 cyber crimes have suggested in the course of the state. Greater than 24000 of these times are registered under the IT Act and the rest beneath the pretty lots of sections of IPC and other State stage Legislations (SLL) (Rakesh Dubbudu ,2016).

The numbers of instances registered beneath the IT Act and IPC have been growing constantly. The instances registered under the IT act grew by way of using more than 350% from 2011 to 2015. There turned into nearly a 70% increase in a number of cyber crimes underneath the IT act among 2013 and 2014. The cases registered under the IPC increased with the resource of greater than 7 times throughout the interval between 2011 and

2015. The identical trend is observed in the number of people arrested. The government moreover acknowledges the expand the number of such crimes and that the creation of implemented sciences, devices along with smart telephones and complex functions, and rise in utilization of cyberspace for corporations has ended in such an expand.

INFORMATION AND CYBER INSECURITY:

The insights on virtual crime in India paint a photograph that none may be glad for. Right now, the digital crimes in India are nearly around 1, 49,254 and can susceptible to move the 3,00000 in the years yet to come, developing at Compounded Annual Growth Rate (CAGR) of around 107 for every penny. According to the discoveries, constantly about 12,456 instances enrolled in India. The managing an account segment maintains on being more inclined to virtual cheats. The styles of misrepresentation might be recommended using PC frameworks, consisting of bank misrepresentation, checking, records fraud, blackmail, and theft of characterized facts. A collection of internet hints, numerous in view of phishing and social building, target consumers and companies (Peter K, 2013).

DEFINITION OF CYBER CRIME:

The expression "cybercrime" has not characterized in any Statute or Act (National Crime Records Bureau Ministry of Home Affairs,2015). The Oxford Reference online characterizes "cybercrime" as a crime perpetrated over the Internet. PC crime, or cybercrime, is a crime that consists of a PC and a device. The PC might also have applied as a part of the commission of against the law, or it might be the target (Amit Kumar, Sharda Avdhanam, 2013). Cybercrimes is an "Offence which is finished against humans or gatherings of humans with a criminal notion manner to intentionally hurt the notoriety of the casualty or reason bodily or mental damage, or misfortune, to the casualty especially or by way of implication, using modern-day media transmission systems, as an instance, Internet (Debarati Halder, 2011). Cyber crime is the crime in which a computer and a network can also be used for the cause. The fundamental element for the boom in cyber crime is the accessibility of the Internet to users even on their mobile phones. Through the usage of Internet, cyber criminals have often indulged in crimes like identification robbery, economic robbery, espionage, pornography, or copyright infringement (James M. Stewart, 2008).

Issues revolving around cyber crime became additional and extra superior. Pc related crook activities have full-grown in importance Associate in Nursing institutions vicinity unit extra interested than ever inputs and finish to those attacks. Progressions are created within the improvement of latest malware package deal, which might also without a doubt find crook behavior (Svensson, P, 2011). Top nice antivirus structures area unit presented free presently with the buy of a laptop or software machine (Balkin, J, 2007).

OBJECTIVES OF THE STUDY

The growing risk from crimes has committed via the Internet, or against statistics on computer systems, is beginning to claim the interest of the sector at huge. This has a look at investigates whether or now not individuals might use the internet to file crime. The essential objective of the have a look at is to discover media recognition among different respondents on the risk of cyber crime.

MATERIALS AND METHODS

Quantitative analysis of the kind of a survey instrument has used to build up the information and descriptive data to investigate the knowledge. Quantitative evaluation technique turned into as soon as used to guide the genuine confirmed reality that the outcomes of the survey have were given to be part of the society who has access to the internet. Because of the character of the evaluation, queries have derived from the literature. These queries supplied a foundation for the analysis of the way to get a transparent opinion about cyber crime among respondents and additionally to find out the kind of cyber crime so happening in the modern day days and what needs to be finished to stop such crimes.

RESULTS

The number one target respondents were working professionals who were aware of diverse PC related crimes and security troubles inside his/her organization. Typically, they included senior managers, IT administrators as well as IT experts. Simple random sampling was the primary sampling approach used when choosing the sample for this survey.

The demographic profile (Table 1) shows the respondents of involved in this study. As per this, out of 100 respondents, majority that is 60% were male and 40% female. With reference to age, 50 per cent fall in the category of 19-24 years, 40% belong to 25-30 age group while the remaining 10% are above30. Regarding the profession, half of the respondents that is, 50% were students and the remaining half were IT professionals. When enquired about the device they use, it was learnt that 18% were using only mobile phone. Laptop or personal computer was used among 7% of the respondents while 57% reported they use laptop and PC as well as mobile whereas the rest 18% are making use of all the devices. Figure: 1 shows the strength of password being used on a computer or mobile. When asked about either active firewall or antivirus was installed in the computers, it was found that most of the users having active antivirus in their computers, 28% to 30% and the very few of them had a very low active firewall in their gadgets.

Regarding updating the software20 to 30% of the people agreed average to very high values respectively. Regarding Wi-Fi use at home, 28, 22, and 18 percent of the people expressed it as average, high and very high values respectively when it comes to safety. Regarding online offers, 15 to 32 per cent of the respondents were of the opinion that indeed it is high.

Table 1: The demographic profile

Criteria		Frequency	Percent	Chi-Square	P value
Age	19-24	50	50%	26.000	0.001**
	25-30	40	40%		
	above 30	10	10%		
	Total	100	100%		
Gender	Male	60	60%	4.000	0.046*
	Female	40	40%		
	Total	100	100%		
Profession	Student	50	50%	0.000	1.000
	IT Professional	50	50%		
	Total	100	100%		
Device Used	Mobile	18	18%	57.840	0.001**
	Laptop or PC	7	7%		
	Laptop or PC and Mobile	57	57%		
	all the above	18	18%		
	Total	100	100%		

Hypothesis:

H1 The distribution of Terrorism is the same across categories of Impact.

H2 The distribution of Safety is the same across categories of Impact.

H3 The distribution of Prevention is the same across categories of Impact.

H4 The distribution of Victimization is the same across categories of Impact.

H5 The distribution of Vandalism is the same across categories of Impact

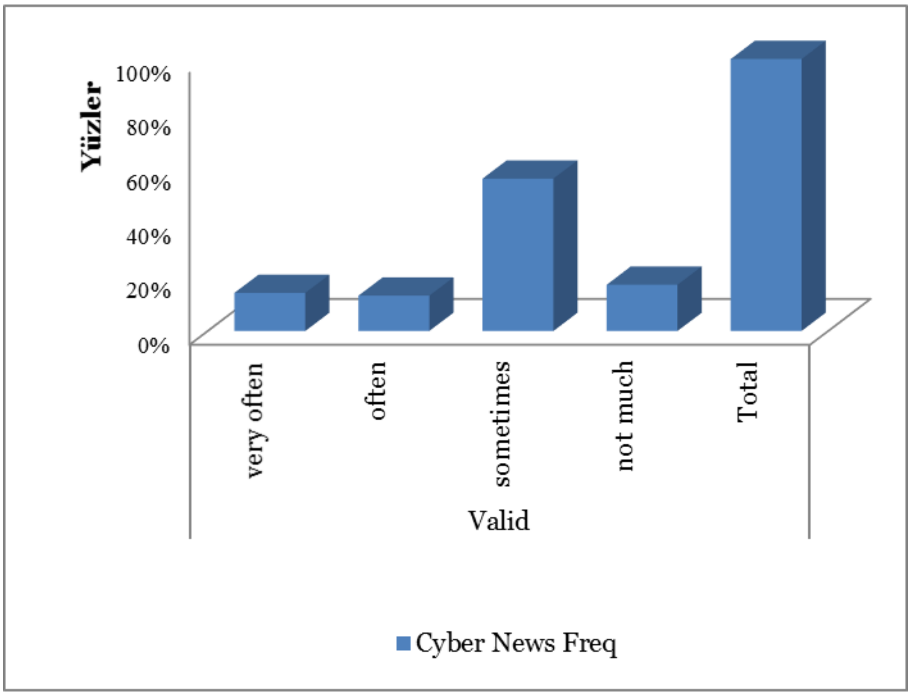


Figure: 2 Cyber Crime Frequency

Figure: 2 shows the frequency of cyber related crime news being presented in the media. For this a majority of the respondents that is 60 per cent felt that only sometimes the media is giving cyber crime related news, 25 per cent said they did not find enough news related to cyber security while only 20 per cent were of the opinion that cyber crime related news appear in media very often.

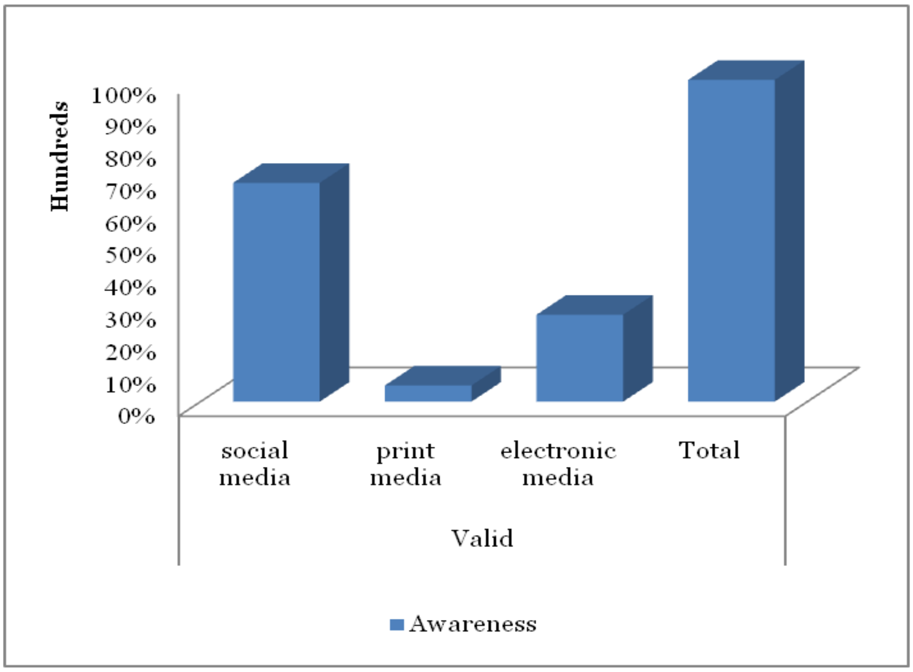
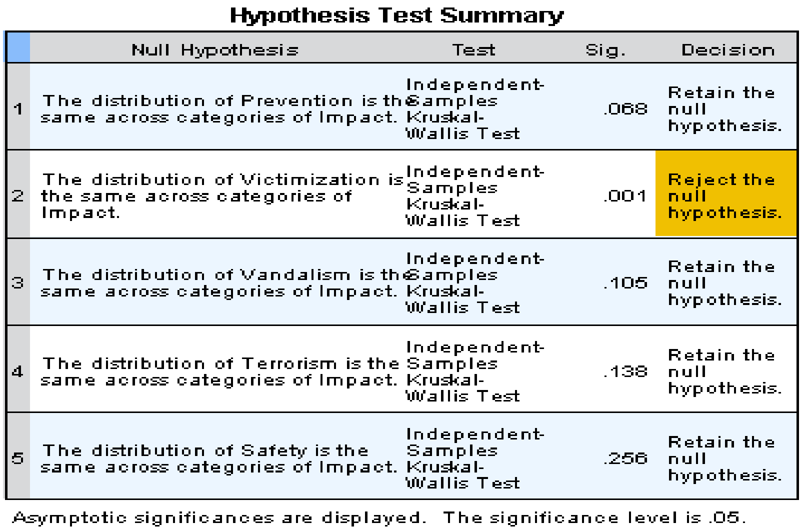


Figure: 3 Media Awareness

Figure: 3 show that most of the respondents that is 80 percent expressed that social media is creating more awareness than print or electronic media. Of the remaining 20 percent, 5 per cent were of the opinion that print media is creating more awareness and 15 per cent said it is the electronic media, which is creating people more aware of on issues related to cyber crime. Hypothesis in fig: 4 victimization of media impact has proved an significant value0.001**.



Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The distribution of Prevention is the same across categories of Impact.	Independent-Samples Kruskal-Wallis Test	.068	Retain the null hypothesis.
2	The distribution of Victimization is the same across categories of Impact.	Independent-Samples Kruskal-Wallis Test	.001	Reject the null hypothesis.
3	The distribution of Vandalism is the same across categories of Impact.	Independent-Samples Kruskal-Wallis Test	.105	Retain the null hypothesis.
4	The distribution of Terrorism is the same across categories of Impact.	Independent-Samples Kruskal-Wallis Test	.138	Retain the null hypothesis.
5	The distribution of Safety is the same across categories of Impact.	Independent-Samples Kruskal-Wallis Test	.256	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Figure: 4 Hypothesis Test

0.001**Reject Null Hypothesis and others have retained Null Hypothesis.

Table:2 ANOVA:

		Sum of Squares	df	Mean Square	F	Sig.
Prevention	Between Groups	1.68	1	1.68	0.24	0.62
	Within Groups	677.07	98	6.91		
	Total	678.75	99			
Victimization	Between Groups	1.04	1	1.04	0.29	0.59
	Within Groups	356.75	98	3.64		
	Total	357.79	99			
.Piracy	Between Groups	8.42	1	8.42	4.43	0.04
	Within Groups	186.22	98	1.90		
	Total	194.64	99			
Terrorism	Between Groups	4.25	1	4.25	8.95	0.004
	Within Groups	46.50	98	.475		
	Total	50.75	99			
Prevention	Between Groups	211.33	1	211.33	2.20	0.14
	Within Groups	9414.62	98	96.07		
	Total	9625.96	99			
Media Impact	Between Groups	56.12	1	56.12	46.05	0.001
	Within Groups	119.43	98	1.22		
	Total	175.56	99			

Significant difference between conditions in table: 2 ANOVA. There used to be a enormous amount of reliability in words remembered at the p<.05 level for the three conditions [F (4, 995) = 4.62, p = 0.001].” There used to be a big outcomes of quantity +of factors on words remembered on the p<.05 stage for the three stipulations [F (4, 995) = 4.47, p = 0.001].” There was a enormous effect of quantity of theory on words remembered at the p<.05 stage for the three stipulations [F (4, 995) = 4.89, p = 0.001]. There was once a massive result of quantity of consumption on words remembered at the p<.05 stage for the three stipulations [F (4, 995) = 3.82, p = 0.004]. There used to be a big outcomes of amount of demands on words remembered at the p<.05 level for the three stipulations [F (4, 995) = 3.30, p = 0.011]. There was once a giant outcome of quantity of requisition on phrases remembered at the p<.05 levels for the three conditions [F (4, 995) = 1.22, p = 0.302] (table: 2 ANOVA).

Table:3 ANOVA with Cochran's Test

		Sum of Squares	df	Mean Square	Cochran's Q	Sig
Between People		1901.01	99	19.20		
Within People	Between Items	156067.15	5	31213.43	472.22	0.001**
	Residual	9182.35	495	18.55		
	Total	165249.50	500	330.50		
Total		167150.60	599	279.05		

Table:4 Multivariate Tests[a]

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	0 .10	6321.93[b]	2.00	55.00	0.001**	0.10
	Wilks' Lambda	0.004	6321.93[b]	2.00	55.00	0.001**	0.10
	Hotelling's Trace	229.90	6321.93[b]	2.00	55.00	0.001**	0.10
	Roy's Largest Root	229.90	6321.93[b]	2.00	55.00	0.001**	0.10
Prevention	Pillai's Trace	0.97	4.84	22.00	112.00	0.001**	0.49
	Wilks' Lambda	0.22	5.71[b]	22.00	110.00	0.001**	0.53
	Hotelling's Trace	2.70	6.63	22.00	108.00	0.001**	0.57
	Roy's Largest Root	2.32	11.81[c]	11.00	56.00	0.001**	0.70
Victimization	Pillai's Trace	0.58	3.81	12.00	112.00	0.001**	0.29
	Wilks' Lambda	0.49	3.90[b]	12.00	110.00	0.001**	0.30
	Hotelling's Trace	0.90	3.10	12.00	108.00	0.001**	0.31
	Roy's Largest Root	0.67	6.28[c]	6.00	56.00	0.001**	0.40
Prevention * Victimization	Pillai's Trace	1.44	5.54	52.00	112.00	0.001**	0.72
	Wilks' Lambda	0.07	5.88[b]	52.00	110.00	0.001**	0.73
	Hotelling's Trace	5.10	6.23	52.00	108.00	0.001**	0.75
	Roy's Largest Root	4.30	9.26[c]	26.00	56.00	0.001**	0.81

a. Design: Intercept + Prevention + Victimization + Prevention * Victimization
b. Exact statistic
c. The statistic is an upper bound on F that yields a lower bound on the significance level.

Table: 3 suggests that A Cochran's Q experiment decided that there used to be statistically a big difference in the proportion of men and women who have crime consciousness over time, $p < .0005$. The multivariate tests (Table: 3) table displays four tests of significance for each model effect. When more than one measure is specified; multivariate tests are computed for between-subjects and within-subjects factors.

The multivariate tests (Table: 4) table displays four tests of significance for each model effect. When more than one measure is specified, multivariate tests are computed for between-subjects and within-subjects factors

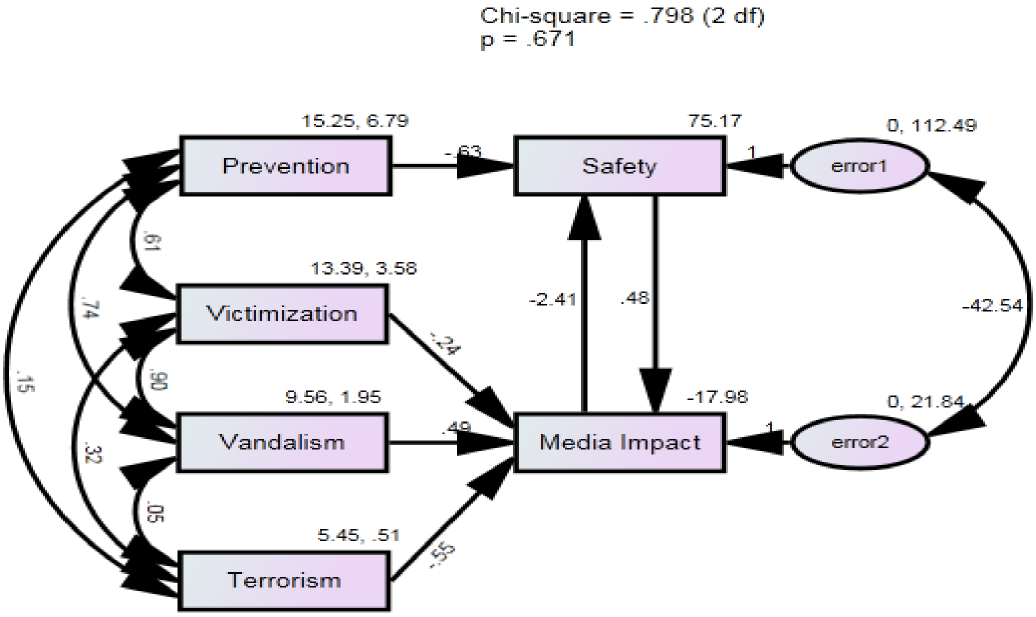


Figure: 5 Structural Equation Model

Table: 5 Means: (Group number 1 - Default model)

Factors	Estimate	S.E.	C.R.	P	Label
Prevention	15.25	0.26	58.24	***	par_14
Victimization	13.39	0.19	70.43	***	par_15
Terrorism	5.45	0.07	76.11	***	par_16
Vandalism	9.56	0.14	68.18	***	par_17

Figure: 5 Structural Equation model and table: 5 exhibit that the likelihood of getting a critical ratio as significant as fifty eight.241 in absolute worth is lower than 0.001. In different words, the imply of prevention is vastly special from no person on the 0.001 degree the likelihood of getting a valuable ratio as massive as 70.434 in absolute worth is not up to 0.001. In other phrases, the mean of Victimization is tremendously distinctive from zero on the zero.001 level. The likelihood of getting is a vital ratio as huge as 76.12 in absolute worth is less than 0.001. In other words, the Mean of Terrorism is greatly different from zero on the zero.001 stage. The likelihood of getting is a critical ratio as colossal as 68.18 in absolute value is lower than 0.001. In other phrases, the mean of Vandalism is vastly different from zero on the 0.001 candidly (two-tailed).These statements are roughly correct for lavish samples underneath compatible assumptions.

MODEL FIT ASSESSMENT

Model fit measures like chi-square/measure of freedom, the comparative match index, root imply rectangular error of approximation, the normative match index, incremental fit index, and the Tucker Lewis index had been used to estimate the measurement model fit.

Table: 6 Model fit Assessment

Indices	Value	Suggested value
Chi-square/degree of freedom (x2/d.f.)	0.797	≤ 5.00 (Hair et al., 1998)
CMIN	0.797	0.001
CFI	1.000`	> 0.90 (Daire et al., 2008)
Goodness of Fit Index (GFI)	0.528	>0.90 (Hair et al. 2006)
Adjusted Goodness of Fit Index (AGFI)	0.832	> 0.90 (Daire et al., 2008
Normated Fit Index (NFI)	0.981	≥ 0.90 (Hu and Bentler, 1999)
Incremental Fit Index (IFI)	1.028	Approaches 1
Tucker Lewis Index (TLI)	1.310	≥ 0.90 (Hair et al., 1998)

The GFI of this gain knowledge of was once 0.528more than the advocated value of 0.90 the other measures equipped satisfactorily; AGFI=zero.832, CFI=1.000, TLI=1.310, IFI=1.028and NFI=0.981with x2/DF < 3 at 2.51 and RMSEA=zero.152 point out a excellent absolute match of the model. Goodness of suits indices help the ultimate fit and these emphasized indices indicate the acceptability of this structural model. For the end of testing the superb match null speculation and substitute hypothesis are framed.

DISCUSSION

Analysis performed on the premise of the KPMG in India's cybercrime survey, 2015, The survey noticed over 250 contributors from the likes of CIOs, CISOs, CAEs, CROs, COOs* and related professionals from across India. While corporations work their manner into designing the most suitable cyber protection plan, considered one of the largest demanding situations faced by most CIOs in defining a strategy is the blurring traces of the IT perimeter of their organizations because of offerings shifting to the cloud, and worker-centric Bring their Own Device rules. This may want to suggest defining strategies based totally on figuring out what statistics is at stake, in preference to basing techniques on what safety equipment the employer is lacking. While placing cyber defense strategies into play, it's far vital for businesses to take attention of the subsequent key insights: Deeper cybercrime hazard assessment: With the constant growth in cybercrime and its impact, it's far vital for groups to identify the crown jewels that need to be protected. With a massive risk landscape and an extensive variety of chance assaults, companies want to reveal their structures (Cybercrime survey report,2015). But this observe of Structural Equation Model Analyzed on Cyber Crime and Media Awareness in India has been in a different way approached and proved social media to create an extra focus on cyber crime prevention with the fairly statistical quantitative evaluation version.

CONCLUSIONS

Lack of consciousness approximately the Internet as a device to Prevent crime changed into revealed. So there's no correlation between the extent of media recognition of the respondents and the underestimation of the cyber crime chance to the community. It can be brought to the fact that it's miles a commonplace misconception. One of the most vital outcomes is the capacity publicity of the population when it comes to the threats of cyber crime. Most of the respondents that are eighty in line with a cent of them are of the opinion that social media is creating focus the various public. How much are we safe, comfortable and reliable on these laptop surroundings? Moreover, not anything is assured. It is important no longer best to our national safety and for the Indian financial system; it's far seemed into as a specific scientific development and the possibility of time and more over now, not a clean venture to address Internet crime as such without proper policy implementations. However, it's miles viable to address such cyber crimes with proper policies and guidelines that need to be carried out by way of the government so that human beings at huge are safer at the cyber area and experience loose to use the Internet anyplace important without any fear. To obtain that object, it's far essential to bring about media focus a number of the public. The survey has analyzed with the aid of the ANOVA test; normative evaluation and Model in shape assessment.

REFERENCES

Balkin, J. M. et al. Cybercrime: digital cops in a networked environment. New York : New YorkUniversity Press (NYU), 2007.

BenBrandt(2011), Terrorist Threats to Commercial Aviation: A Contemporary Assessment. https://www.ctc.usma.edu/posts/terrorist-threats-to-commercial-aviation-a-contemporary-

Cybercrime survey report (2015) KPMG, an Indian Registered Partnership and a member firm of the KPMG network https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/

Debarati Halder and Jaishankar, K. (2011)Cybercrime,https://en.wikipedia.org/wiki/ Cybercrime, ,

James M. Stewart, Ed Tittel, Mike Chapple.CISSP: Certified Information Systems Security Professional Study Guide. indiana : wiley publishing ing, 2008. 9780470276884.

Janna Anderson and Lee Rainie (2014) Net Threats http://www.pewinternet.org/2014/07/03/net-threats/.

National Crime Records Bureau Ministry of Home Affairs. New Delhi : s.n., 2015.

Peter K. Analysis of intellectual property issues. yu., 1, new : The WIPO Journal is a peer reviewed journal., 2013, Vol. 5.

Rakesh Dubbudu (2016) Cyber Crimes in India: Which state tops the chart?.https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/.

Svensson, P. asdaq hackers target service for corporate boards. [Online] 2011. http://news.yahoo.com/s/ap/20110205/ap_on_hi_te/us_nasdaq_hackers .

Symantec .Internet security Threat Report 2014. USA : Symantec Corporation.

Vinit Kumar Gunjan ; Amit Kumar ; Sharda Avdhanam (2013), A survey of cyber crime in IndiaPublished in: Advanced Computing Technologies (ICACT), 15th International Conference on 21-22 Sept. 2013 DOI: 10.1109/ICACT.2013.6710503, IEEE