

Cyber Crime and Media Awareness in India

¹Dr.R.Praba, ²Sedhuvignesh M, ³Rathinasamy T, ⁴Madhan Kumar S

Department of Information Technology

Dr. N. G. P. Arts and Science College, Coimbatore, India

Abstract: The prevalence of cyber-related crimes involving computer and mobile phone use has been on the rise in India, raising concerns about the need to protect information systems from unauthorized dissemination and removals. Cyber security teams have been kept on their toes due to incidents such as hacking, theft of data, cyber bullying, and cyber extortion. The majority of respondents (60%) reported that they only occasionally receive cyber crime-related news from the media, with 25% reporting that they do not find enough cyber-related news in the media and 20% reporting that cyber-crime-related news appears in the media on a regular basis. Out of the remaining 20%, 5% reported that print media was creating more awareness, while 15% reported that it was the electronic media which was creating more awareness on cyber-related issues. The qualitative analysis of the survey style enabled the collection of information which was analyzed through the use of ANOVA tests, multivariate tests, normative analysis, structural equation model, and model fit assessment. Measures being taken to combat cybercrime are also discussed.

Keywords: Cybercrime; Law; Internet Crime; Structural Equation Model and Media Awareness

INTRODUCTION

India is one of the most populous countries in the world, and the rise in crime is a major concern for the nation's economy and the Indian government. Computer-based cyber crimes are on the rise, posing a greater risk to the nation's security. Computers are a fundamental part of modern life, and the sheer number of individuals who have access to information stored on computers, as well as the majority of commercial and governmental data, presents a serious threat. To protect information systems from unauthorized dissemination, it is essential to ensure that they are not tampered with or removed without permission. Unfortunately, the cyber security community has been kept on its toes by the increasing number of incidents, from hacking and data theft to cyber bullying and cyber extortion. Unfortunately, website developers, internet and networking software experts are barely

able to contain this menace. These violations can have a detrimental effect on a nation's security, and the money-related wellbeing issues associated with these types of crimes have become increasingly prominent, particularly those involving hacking, copyright infringement, erotic entertainment and child preparation.

INFORMATION AND CYBER INSECURITY

India's digital crime statistics reveal a picture that no one can be happy about. Currently, the number of digital crimes in the country stands at around 1.49,254, and is on the verge of crossing the 3,000,000 mark in the next few years, with a CAGR of approximately 107 for every penny. According to the findings, there are around 12,456 registered cases in India each year. The segment of managing an account continues to be the most vulnerable to digital scams. Types of misrepresentation that can be facilitated through PC frameworks include bank misrepresentations, checking fraud, data fraud and blackmail, and the theft of classified data. Various web tricks, many of which are targeted at shoppers and organizations, are used for phishing, social building, etc.

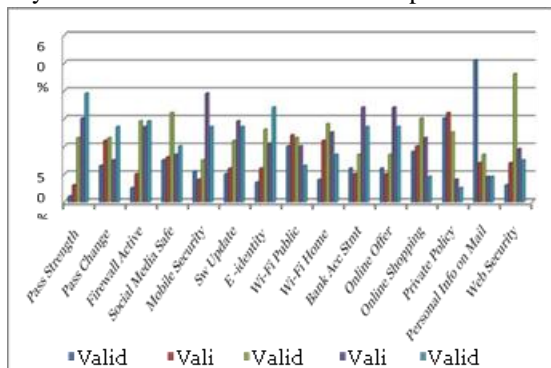
DEFINITION OF CYBER CRIME

The concept of cybercrime has not been formally defined in any statute or law. However, the Oxford Reference online defines cybercrime as a crime committed over the internet. PC crime is a crime that involves a computer and a system, where the PC may have been used as a means of committing a crime or may have been the target of the crime. Cybercrimes are defined as an offence that is committed against individuals or groups of individuals with a criminal mindset with the intention of deliberately damaging the reputation of the victim or causing physical or mental harm or misfortune to the victim, either directly or indirectly, through the use of modern media

transmission systems, such as the Internet. The primary contributor to the rise in cybercrime is the availability of the Internet, which has enabled cybercriminals to commit crimes such as identity theft, financial fraud, espionage, pornography and copyright infringement.

METHODOLOGY

Within the range of a survey tool, quantitative analysis has been employed to gather the knowledge and descriptive data to explore the comprehension. The methodology of quantitative analysis was initially employed to support the well-established fact that the respondents of the survey must be members of the society that has access to the internet. Due to the nature of the assessment, questions have been extracted from the literature. These questions provided a basis for the analysis to gain a clear understanding of the respondents' opinion on cyber crime and to know the type of cyber crime that is happening in the last few days and what needs to be done to stop such crimes.



MODEL FIT ASSESSMENT

Measurement model fit measures such as chi-square / measure of freedom, comparative match index, root imply rectangle error of approximation, normale match index, incremental fit index, and tucker Lewis index were used to estimate the model fit. This gain knowledge of the GFI is once 0.528 more than the advocated value (0.90). The other measures fit satisfactorily: AGFI = 0.832, CFI = 1.000, TLI = 1.310, IFI = 1.028, NFI = 0.981 with $\chi^2 / DF < 3 = 2.51$, RMSEA = 0.152 indicating an excellent absolute fit of the model. The goodness of suits indices help in the final fit. These emphasized indices help in the acceptability of the structural model. End of testing

superb match null hypothesis and substitute hypothesis

MODEL FIT ASSESSMENT

Indices	Value	Suggested value
Chi-square/degree of freedom ($\chi^2/d.f.$)	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)

CONCLUSION

The lack of awareness of the Internet as an instrument to prevent crime was also revealed. Therefore, there is no link between the media awareness of respondents and the under-estimation of the threat of cyber crime to the society. It can be concluded that this is a common misperception. One of the most significant results is the possible exposure of the society in relation to cyber crime threats. Eighty percent of respondents believe that social media creates awareness among the population. How secure, safe and reliable are we in this computer world? And nothing is secure. It is not only important for our national security, but also for the economy of India. It is considered as a separate scientific development and it may take more time and more than expected to deal with internet crime as such. Without proper policy implementation, it will not be an easy task.

REFERENCE

- [1] Janna Anderson and Lee Rainie (2014) Net Threats <http://www.pewinternet.org/2014/07/03/net-threats/>.
- [2] Ben Brandt(2011), Terrorist Threats to Commercial Aviation: A Contemporary Assessment. <https://www.ctc.usma.edu/posts/terrorist-threats-to-commercial-aviation-a-contemporary-assessment>.
- [3] National Crime Records Bureau Ministry of Home Affairs. New Delhi : s.n., 2015.
- [4] Symantec .Internet security Threat Report 2014. USA : Symantec Corporation. , 2014.
- [5] Vinit Kumar Gunjan ; Amit Kumar ; Sharda

- Avdhanam, A survey of cyber crime in IndiaPublished in: Advanced Computing Technologies (ICACT), 2013 15th International Conference on 21-22 Sept. 2013 DOI: 10.1109/ICACT.2013.6710503, IEEE
- [6] Rakesh Dubbudu (2016) Cyber Crimes in India: Which state tops the chart?. <https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/>.
- [7] Analysis of intellectual property issues. yu., Peter K. 1, new: The WIPO Journal is a peer reviewed journal., 2013, Vol. 5.