IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A STUDY ON CHALLENGES FACED BY OFFICERS INVESTIGATION OF CYBERCRIME CASES IN CHENNAI

[1]Mr. Aravindan E., [2]Mr. Bhuvaneshwari G.

[1]Student,[2]Assistant Professor

School of Business Administration

Sathyabama Institute of Science and Technology, Chennai-600119, India.

Abstract: Cybercrime encompasses any criminal act dealing with computers and networks. It includes crime conducted through the Internet. The Internet is basically the network of networks used across for communication and sharing of data. Cybercrime also known as the computer crime is the use of an instrument for illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. With the advancement of the Internet technologies like the 2G and 3G, the global village is effectively sharing and communicating vital data(s) across the network. However, there are some who are intentionally trying to track and extract the vital and confidential information illegally for their personal use or for the financial achievement and many more. The generic aim of this study was to profile the nature, content, type, frequency, intensity and extensity of job satisfaction for various cadres of cyber-crime professionals belonging to a major city of south India as well as in relation to associated personal socio-demographic variables. A subsidiary aim was also to determine the reliability and validity of the instrument being used for measurement of job satisfaction in the targeted population of police personnel. First, staff report there has been an escalation and acceleration of the quantity of the work cyber-crime units are expected to undertake. Second, the resourcing of cyber-crime units has not developed commensurate with the increasing demands. These three major themes emerged in both of the case study sites; however, there were some differences between the two sites that will be explored later. Following a discussion of these three categories of findings, we consider various suggestions made by staff for how to improve this situation. The paper concludes by highlighting the significance of the findings for the capabilities of police cyber-crime units and calls for further empirical research into police responses to cyber-crime.

I. INTRODUCTION

Computer crime, or Cybercrime, refers to any crime that involves a computer and a network. Net crime is criminal exploitation of the Internet. Issues surrounding these types

of crimes have become high-profile, particularly those surrounding cracking, copyright infringement, child pornography, and child grooming. There are also problems of privacy when confidential information is lost or intercepted, lawfully or otherwise. Cyber-crime is an escalating priority for national and international police and security agencies.Similar upward trajectories of the threat and costs of cyber-crime can be found all across the globe. Research has continued to emphasise the complexities associated with preventing and responding to cyber-crime, including the complex dynamics of cyber- crime networks and the need for effective transnational security networks to respond to cyber-crime. However, despite the growing social and economic costs of cyber-crime, it seems evident that the main beneficiaries of increased public-sector funding to promote cyber security have been security and intelligence agencies rather than local police organisations. The key questions behind this research are: what are the key challenges facing specialist cyber-crime units and according to members of these units, what are the key changes needed to strengthen police responses to the escalating threat of cyber- crime? Three clear themes emerged from the data.

II. LITERATURE REVIEW

Ciancaglini et al. (2013) crawling into that unreachable area and explaining things in a more realistic light identified the deep web as any online content that cannot be indexed by search engines, including dynamic web pages, blocked sites, unlinked sites, private sites with login credentials, non- HTML/-contextual/-scripted content, and limited-access networks. **Jaishankar (2018)** illustrated that many researchers who attempted to address the causation of cyber-crimes with traditional theories (such as social learning theory, routine activities theory and drift and neutralization theory) were not fully successful in their explanation of cyber-attacks. For that reason, the space transition theory was propounded by the author himself. **K. Choi., & C. S. Lee. (2018)**, Cyber criminology combines knowledge from criminology, psychology, sociology, computer science, and cyber security, to provide an in-depth understanding of cybercrime. Cybercrime and cyber security are interconnected across many places, platforms, and actors. **Karamchand Gandhi (2012)**, Cybercrime is emerging as a serious threat. Worldwide governments, police departments and

intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel.

III. RESEARCH METHODOLOGY

The research design adopted for this study is Exploratory Research. A sampling design is a definite plan for obtaining a sample from a given population. It refers to the technique adopted by the researcher in selecting items for the sample. Simple random sampling is used. It is a single element or group of elements subjected to selection in the sample. Here in this project, the sampling unit is police officers working for cyber-crime department and its size are 145.Area of survey is Chennai After the data has been collected, analysis is made from questionnaire and tabulation method is followed. Tabulation is a technique procedure where in data is classified and put in the form of tables. The tables thus obtained were analyzed with statistical tools like percentages and pie diagram so that interpretation would be precise and easy.

IV. DATA ANALYSIS

The data analysis for the survey is carried out with the percentage analysis, Chi-Square test and one way ANOVA test. They are illustrated and explained in the following

4.1 One Way ANOVA

Null Hypothesis:

Ho = There is no significant difference between Age and Working as a Team is not a Problem.

Alternate Hypothesis:

H1 = There is a significant difference between Age and Working as a Team is not a Problem.

TABLE-1. SHOWING AGE AND WORKING AS A TEAM IS NOT A PROBLEM

ANOVA

WORKING AS A TEAM IS NOT A PROBLEM

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	50.815	4	12.704	19.292	<.001
Within Groups	92.192	140	.659		
Total	143.007	144			

The p-value is 0.001 which is lesser than the alpha value (0.05), hence alternate hypothesis (H1) is accepted. Therefore, there is a significant difference between Age and Working as a Team is not a Problem.

4.2 Chi-Square Test

Null hypothesis (Ho): There is no significant difference between Role immediately prior to joining the Cyber-Crime unit and Job is interesting & prospective.

Alternate hypothesis (H1): There is a significant difference between Role immediately prior to joining the Cyber-Crime unit and Job is interesting & prospective.

TABLE-2. SHOWING ROLE IMMEDIATELY PRIOR TO JOINING THE CYBER-CRIME UNIT AND JOB IS INTERESTING & PROSPECTIVE

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	389.195[a]	16	<.001
Likelihood Ratio	304.915	16	<.001
Linear-by-Linear Association	56.196	1	<.001
N of Valid Cases	145		

a. 16 cells (64.0%) have expected count less than 5. The minimum expected count is .07.

The p-value is 0.001 which is lesser than the alpha value (0.05), hence alternate hypothesis (H1) is accepted. Therefore, there is a significant difference between Role immediately prior to joining the Cyber-Crime unit and Job is interesting & prospective.

IV. SUGGESTION

Protection against cybercrime starts at taking personal measures for protection and then escalates to organizational, societal, corporate, national, military and international levels. Defense in depth of cyber security at all levels will minimize, prevent and decelerate cyber-attacks. Technology by itself is not enough, the integration of other fields like training; awareness, social aspects, culture, laws, prosecution and international cooperation are needed to blend with technical solutions to tackle cybercrime. Creation of satisfied work-force can lead this activity. From the study findings, we can recommend the following suggestions to the police officers working for cyber-crime branch,

V. CONCLUSION

From this study, it has been found that there are many ways and means through which an individual can commit crimes on cyber space. Cyber-crimes are an offense and are punishable by law and how cyber-crime officers might effectively recruit a diverse, talented workforce and retain those officers once hired. Satisfied police officers are the one who work with passion and feel a profound connection to their organization. They drive innovation and move the organization forward. From the study results shows that police officers working on Cyber-crime branch are satisfied with the interpersonal relationship, working condition, welfare and

benefits and communication from the top management. Nevertheless, the dissatisfaction expressed by few of them also has to be taken in to consideration. An all-round pleasing, conducive environment creates better public relations as well as happier human relations.

REFERENCES

[1] Ciancaglini, V., Balduzzi, M., Goncharov, M., & McArdle, R. (2013). Deepweb and Cybercrime, Trend micro report.

[2] Jaishankar, K. (2018). Cyber Criminology as an Academic Discipline: History, Contribution and Impact. International Journal of Cyber Criminology, 12(1), 1-8.

[3] K. Choi., & C. S. Lee. (2018). International Journal of Cybersecurity Intelligence and Cybercrime, 1 (1), 1-4.

[4] Karamchand Gandhi (2012), An Overview Study on Cyber-crimes in Internet, Journal of Information Engineering and Applications, ISSN 2224- 5782 (print) ISSN 2225-0506, Vol 2, No.1, 2012

[5] Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies, Third World Quarterly, 31(7), 1057-1079.