

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

Submitted in partial fulfillment of the requirements for the award of

Master of Business Administration

by

ARAVINDAN E

Register No.39410022



SCHOOL OF BUSINESS ADMINISTRATION

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with Grade "A" by NAAC | 12B Status by UGC | Approved by AICTE

Jeppiaar Nagar, RAJIV GANDHI SALAI, CHENNAI - 600 115.

April - 2021



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Accredited with "A" grade by NAAC | 12B Status by UGC | Approved by AICTE

Jeppiaar Nagar, Rajiv Gandhi Salai, Chennai – 600 119

www.sathyabama.ac.in

SCHOOL OF BUSINESS ADMINISTRATION

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **ARAVINDAN E (39410022)** who have done the Project work entitled "**A STUDY ON CHALLENGES FACED BY OFFICERS IN INVESTIGATION OF CYBERCRIME CASES IN CHENNAI**" under my supervision from **January 2021** to **March 2021**.

Internal Guide

External Guide

Dr. BHUVANESWARI G.

Dr. BHUVANESWARI G.

Dean – School of Business Administration

Submitted for Viva voce Examination held on _____.

Internal Examiner

External Examiner

(Name in Capital Letters

(Name in Capital Letters

with signature)

with signature)

DECLARATION

I **ARAVINDAN E, (39410022)** hereby declare that the Project Report entitled “**A STUDY ON CHALLENGES FACED BY OFFICERS IN INVESTIGATION OF CYBERCRIME CASES IN CHENNAI**” done by me under the guidance of **Dr. BHUVANESWARI G**, is submitted in partial fulfillment of the requirements for the award of Master of Business Administration degree.

DATE:

PLACE:

SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to Board of Management of **SATHYABAMA** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my sincere thanks to **Dr. BHUVANESWARI G.**, Dean, School of Business Administration and **Dr. PALANI A.**, Head, School of Business Administration for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. BHUVANESWARI G**, for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the School of Business Administration who were helpful in many ways for the completion of the project.

ARAVINDAN E

TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ABSTRACT	i
	LIST OF TABLES	ii
	LIST OF CHARTS	iii
1	INTRODUCTION	
	1.1 Introduction	1
	1.2 Industry profile	2
	1.3 Problem statement	5
	1.4 Objectives of the Study	5
	1.5 Need for the Study	5
	1.6 Scope of the Study	6
2	REVIEW OF LITERATURE	
	2.1 Review Of Literature	7
	2.2 Theoretical Background of the Study	16
3	RESEARCH METHODOLOGY	
	3.1 Type of Project	21
	3.2 Sources of Data	21
	3.3 Sampling Design	22
	3.4 Tools and Techniques	22
	3.5 Limitations of the Study	22
4	DATA ANALYSIS AND INTERPRETATION	
	4.1 Descriptive Analysis – Percentage Method	23
	4.2 Correlation Analysis	51
	4.3 CHI – Square	53
	4.4 Anova	55
	4.5 Regression Analysis	57
5	FINDINGS, SUGGESTIONS AND CONCLUSION	
	5.1 Finding of the Study	58
	5.2 Suggestions	62
	5.3 Conclusion	64
	REFERENCES	65
	APPENDIX Questionnaire I	66
	APPENDIX ARTICLE II	68

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. Third, the level of skills and training within units is often not sufficient to address the nature and growing complexities of investigating cyber-crime, which can lead to disproportionate pressure on the small number of tech-savvy staff present within specialist units. 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.

Key words: Cybercrime, committing fraud, trafficking in child pornography and intellectual property profile the nature, content, type, frequency, intensity and extensity

LIST OF TABLES

Table	Particular	Page No
4.1.1	Educational Qualification of the Respondents	23
4.1.2	Age Of The Respondents	24
4.1.3	Work Experience Of The Respondents	25
4.1.4	Income Level Of The Respondents	26
4.1.5	Role Immediately Prior To Joining the Cyber- Crime Unit	27
4.1.6	Circumstance Through They Joined The Cyber-Crime Unit	28
4.1.7	Comfortable With The Working Hours	29
4.1.8	Job Is Interesting And Prospective	30
4.1.9	Feeling Proud To Be A Part Of Cyber-Crime Department	31
4.1.10	Satisfaction With The Work Hours And Shifts	32
4.1.11	Job Is Affecting The Health	33
4.1.12	Physical Working Conditions	34
4.1.13	Work Place Is Less Crowded And Clean	35
4.1.14	Work Environment Gives Less Emphasis On Equipment	36
4.1.15	Environment Is More Adaptable And Comfortable	37
4.1.16	Health Is Not Neglected Due To Job	38
4.1.17	Time And Energy Spent On Job Won't Affect Health Adversely	39
4.1.18	Necessary Safety Equipment Are Provided By The Cc Department	40
4.1.19	Satisfaction With The Department's Welfare Policies	41
4.1.20	Compensation Earned Helps To Maintain Socially Desirable	42
4.1.21	Satisfaction With Reward System Of Cyber-Crime Department	43
4.1.22	Co-Operation With Co-Officers	44
4.1.23	Working As Team Is Not A Problem	45
4.1.24	Officers' Interact In Terms Of Ideas And Feelings	46
4.2.1	Satisfaction With The Clarity In Communication By Superior	47
4.2.2	Satisfaction With Grievance Handling By Superior	48
4.3.1	Level Of Job Involvement Is High	49
4.3.2	Satisfaction With The Performance Appraisal	50
4.4.1	Satisfaction With The Work Load	51

LIST OF CHARTS

Table	Particular	Page No
4.1.1	Educational Qualification of the Respondents	23
4.1.2	Age Of The Respondents	24
4.1.3	Work Experience Of The Respondents	25
4.1.4	Income Level Of The Respondents	26
4.1.5	Role Immediately Prior To Joining the Cyber- Crime Unit	27
4.1.6	Circumstance Through They Joined The Cyber-Crime Unit	28
4.1.7	Comfortable With The Working Hours	29
4.1.8	Job Is Interesting And Prospective	30
4.1.9	Feeling Proud To Be A Part Of Cyber-Crime Department	31
4.1.10	Satisfaction With The Work Hours And Shifts	32
4.1.11	Job Is Affecting The Health	33
4.1.12	Physical Working Conditions	34
4.1.13	Work Place Is Less Crowded And Clean	35
4.1.14	Work Environment Gives Less Emphasis On Equipment	36
4.1.15	Environment Is More Adaptable And Comfortable	37
4.1.16	Health Is Not Neglected Due To Job	38
4.1.17	Time And Energy Spent On Job Won't Affect Health Adversely	39
4.1.18	Necessary Safety Equipment Are Provided By The Cc Department	40
4.1.19	Satisfaction With The Department's Welfare Policies	41
4.1.20	Compensation Earned Helps To Maintain Socially Desirable	42
4.1.21	Satisfaction With Reward System Of Cyber-Crime Department	43
4.1.22	Co-Operation With Co-Officers	44
4.1.23	Working As Team Is Not A Problem	45
4.1.24	Officers' Interact In Terms Of Ideas And Feelings	46
4.2.1	Satisfaction With The Clarity In Communication By Superior	47
4.2.2	Satisfaction With Grievance Handling By Superior	48
4.3.1	Level Of Job Involvement Is High	49
4.3.2	Satisfaction With The Performance Appraisal	50
4.4.1	Satisfaction With The Work Load	51

CHAPTER 1

INTRODUCTION

1.1 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. An Australian nationwide survey conducted in 2006 found that two in three convicted cyber-criminals were between the ages of 15 and 26.

Cyber-crime is an escalating priority for national and international police and security agencies. The most recent threat report by the Australian Cyber Security Centre, for example, notes that 'malicious cyber activity against Australia's national and economic interests is increasing in frequency, scale, sophistication and severity', with estimates suggesting the total costs of cyber-crime to be well above \$1AU billion per year. Similar upward trajectories of the threat and costs of cyber-crime can be found all across the globe. As DuPont (2017) notes, some of the higher estimates of the costs of cyber-crime tend to approach \$1000US billion. Research has continued to emphasize 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 organizations.

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.

1.2 INDUSTRY PROFILE

Over the last couple of years, increased cyber threats had forced several Indian enterprises to increase spending in tech security between 20 per cent and 35 per cent, said sector officials. India is third in terms of internet users. Its internet protocol (IP) traffic would grow six fold from 2012 to 2017 at a compound annual growth of 44 per cent, said a KPMG report. Due to this, the spend would depend more on the business model rather than size of the company, said some officials.

In 10-15 years, investment in cyber security has remained focused on threat prevention rather than detection and solution. But where the threats are getting more advanced, implementation of a stronger security system has made its way to the priority list of companies.

Erecting Firewall

- Investment in cyber security has remained focused on threat prevention rather than detection and solution
- Indian market for security infrastructure and services growing to \$1.4 billion by 2017 from \$989 million this year
- Attacks like advanced persistent threats or distributed denials-of-service (DDOS) seem the highest in six months
- India's internet protocol traffic is forecast to grow at a compound annual growth of 44% from 2012 to 2017
- Due to heavy net usage, the spend will depend more on the business model than size of the company
- E-commerce, which relies heavily on online services, is among the reactive segments for cyber security

Over two years, security spend has risen between 20 per cent and 35 per cent in India, Sanjoy Sen, senior director at Deloitte India, said. "Indian enterprises have looked at technology as well as non-technological holes to address the threat issue."

IT research and advisory company Gartner also sees the Indian market for security infrastructure (software and hardware) and services (consulting, MSS, implementation and support) together growing to \$1.4 billion by 2017 from \$989 million this year.

"There is no way that you can prevent every threat. In India, most enterprises have predominantly spent towards preventive measures like Firewall in the past," said Ambarish Deshpande, managing director, India, Bluecoat Systems.

"Since the industry has now matured, it (the industry) is expected to focus on spending towards more enhanced tools to tackle advanced cyber threats. Detecting the threat, analyzing it and then spend good amount of intelligence to remove it. This is what will drive the IT security spending growth," Deshpande added. "It is expected to grow exponentially in coming years," he said.

Attacks like advanced persistent threat or distributed denial-of-service (DDOS) seemed to be among toppers for the last six months, said industry officials. "We are seeing different kinds of threats, which have also been on the rise targeting organizations or businesses with varied intentions," said Sidharth Pisharoti, country sales head of India at security solutions company, Akamai Technologies. "Since most of these are well-planned and targeted attacks, an advance damage control system has to be in place." Though most industry officials remained unanimous regarding the increase in IT security spend by Indian enterprises, the view on the spending pattern varied.

"The overall spending figure on IT security will vary from vertical-to-vertical and depend on the extent of security implementation," said Sen of Deloitte India. "Most importantly, it will have to be aligned with the risk involved in the business and is seen proportionate to the rise in risk and growth involved in the business," Sen added. "Spending is expected to increase from top organizations like the Fortune 100 or Fortune 500 companies across all verticals," said Deshpande of security solutions company Bluecoat. "Companies, which have something of their own like intellectual property or money, that can cause heavy damage to their business are being targeted. The intention is to put the organization out of league," he said.

"Those businesses, which have higher dependency on internet like e-commerce or those with sensitive information such as BFSI, telecom, or the government, will see security spend on high priority," Pisharoti said. "Though the spend might not be as drastic as double in coming years, increase is surely there and will depend on the

industry or the individual company as to what is its threat perception,” he added. With the IT security spends on a gradual rise since the last two years, there have been some sectors that have proactively invested towards implementation of security, while some still need to buck up.

“The banking sector has always been proactive towards IT security spend and will continue to be so, given the sensitivity of information we handle,” said a top ICICI Bank official. “Apart from increase in threat perceptions for this sector — internal as well as external — sophistication is also increasing (in the sector) and due to this we see (IT security spend) budgets increasing going ahead,” he added. The auto segment too is looking at increased spend going ahead.

“There is immense scope for automation in the auto sector and so with flexibility going up, even threat perception will go up. This will take the IT security spends proportionately higher in the sector in coming years,” said Jayant Magar, vice-president, IT & CIO, AMW Motors. “The spend has already been on the rise in this sector by about five per cent every year and going ahead too it might rise by same percentage annually,” Magar added. “Telecom is a saturated market and competition is high. So security spend is certainly crucial for the sector and is seen only going upwards in coming years,” said Manoj Shahane, senior manager at Vodafone Shared Services.

“In the electrical segment, computerization is at an initial stage and so security spend, though exists, is at a very nascent stage, less than one per cent of the total revenue,” said G Sowmiya Narayana, general manager (IT-Infrastructure), Bajaj Electricals. Though various sectors are at different stages of security spend and implementation, e-commerce, which relies heavily on online services is among the reactive segments for cyber security. “The e-commerce industry could have been a little bit more proactive towards implementing security solutions,” said Sidharth. “Security solutions were always there not that they have come up now.”

On the other hand, the government though a little slow does not compromise on security spend due to the sensitivity of data it has, officials said. “It (the government) makes sure that they invest in the best technology,” added Pisharoti. Gartner has seen a keen interest from enterprises in India on enhancing their security operations

capabilities to protect their organizations from advanced targeted attacks. “Increased security threats from activists and cyber-crime syndicates have caused more enterprises to re-look at their monitoring, incident response and forensics abilities,” principal research analyst Sid Deshpande at Gartner said. All in all, the major sectors in the domestic market are active and no one is reactive in nature anymore. As increased threats are now a reality, companies know they have to act.

1.3 PROBLEM STATEMENT

Cyber-crime is the new challenge for the Indian society, industry and the law enforcement and the entire criminal justice system as a whole. The anonymous nature of the Internet makes it an attractive medium to commit crimes and frauds. Cyber-crime is not confined to any national boundary. The Police personnel, the prosecutors and the lower judiciary need to be educated to fight cyber-crimes. This can be effectively achieved by organizing periodic conferences, seminars and workshops, training programs. Sometimes we often wonder how wired connected we are with each other. Almost everything in our life is connected to some kind of technology and its gadgets. But imagine what a hacker can do to our life. The Commission on Crime Prevention and Criminal Justice (CCPCJ) of the United Nations, with its headquarters in Vienna, has been exercised over how to prevent and control high technology and computer-related crime. The Commission is convinced that one way of doing this is to forge closer links between nations so that the cyber-criminal is relentlessly pursued across frontiers.

1.4 OBJECTIVES OF THE STUDY

- To identify the challenges faced by officers investigating cyber-crime.
- To define types of cyber-crime against individuals.
- To analyze the factors involved in cyber-crime reporting and investigation.
- To identify the level of job satisfaction of officers working in cyber-crime cells.
- To analysis the level of skills of the officers working in cyber-crime cells.

1.5 NEED FOR THE STUDY

This research aims to determine how police officer satisfaction, retention, loyalty influence the cyber-crime department and performance of police officers working in Cyber –criminality department in Tamil Nadu Police Department. This report intends to prove, that satisfied officers tend to be loyal and committed to the department and it has a positive influence towards the performance of Cybercrime branch. The results would reveal that the increase of job satisfaction makes their intention to continue their work with complete satisfaction

1.6 SCOPE OF THE STUDY

The study was initiated after securing permission from the Commissioner of Police, cyber-crime. To ease test administration, the questionnaire was subjected to reverse translation in regional language orally. Respondents were explained any test item for which clarification was sought. No time limit was prescribed to complete the tool. The instruments chosen for this study was then distributed to consenting and eligible respondents after explaining its rationale in their respective police station limits. The base data collected were individual response sheets of the participating police personnel across each item on the designated tool. They were then coded and tabulated in excel spread sheets before attempting appropriate statistical treatments and analysis

CHAPTER 2

REVIEW OF LITERATURE

2.1 LITERATURE REVIEW

Cybercrime, a concept which to date has defied a globally accepted definition, appears to be the latest scourge plaguing man and same has occupied the cynosure. The word “cybercrime” is on the lips of almost everyone involved in the use of the computer and Internet, be it individual, corporate, organization, national, multinational or international. The attention accorded cybercrimes is not farfetched; on one hand, it is partly rooted in its unavoidable nature as a result of the fact that telecommunications via the cyberspace, is the veritable means by which social interaction, global trade and commerce are transacted; and on the other, the economic losses to which all citizens are exposed whether now or in the nearest future. Aside economic losses, other consequences of cybercrimes includes but not limited to setback to the brand image and company reputation otherwise known as goodwill, loss of intellectual property and sensitive data, opportunity costs which includes but not limited to service and employment disruptions, penalties and compensatory payments to affected clienteles, contractual compensation for delays, cost of countermeasures and insurance, cost of mitigation strategies and recovery from cyber-attacks, the loss of trade and competitiveness, distortion of trade and job loss. This paper argues that it is not as if relevant laws and regulations are not in place because some advanced nations in the world have in one form or another, laws against cybercrimes, yet, the challenge of cybercrimes remains intractable and bewildering. As nations across the globe strives to curb cybercrimes through the instrumentality of the law, so are the cyber criminals devising new and sophisticated techniques to further their trade, thereby rendering impotent, the extant legal measures. This Article intends to bring to the fore, a comprehensive account of why cybercrimes remains an albatross in order showcase the enormity of the challenge faced by humanity, in the hope that, when the extent of the problem is known, may be, a global solution would timeously be fashioned out, to stem the tide of cybercrimes.

Source: Ajayi (2016), Challenges to enforcement of cyber-crimes laws and policy, Journal of Internet and Information Systems, Vol. 6(1), pp. 1-12, August 2016

Cybercrime is a significant challenge to society, but it can be particularly harmful to the individuals who become victims. This chapter engages in a comprehensive and topical analysis of the cybercrimes that target individuals. It also examines the motivation of criminals that perpetrate such attacks and the key human factors and psychological aspects that help to make cybercriminals successful. Key areas assessed include social engineering (e.g., phishing, romance scams), online harassment (e.g., cyber-bullying, trolling, revenge porn, hate crimes), identity-related crimes (e.g., identity theft, doxing), hacking (e.g., malware, crypto jacking, account hacking), and denial-of-service crimes. As a part of its contribution, the chapter introduces a summary taxonomy of cybercrimes against individuals and a case for why they will continue to occur if concerted interdisciplinary reports are not pursued.

Source: Jason R. C. Nurse (2018), *Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit*, *The Oxford Handbook of Cyber psychology* (2018/19)

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. Cybercrime issues are continuously and expeditiously changing and developing, especially with the advent of new technologies. The International Journal of Cyber security Intelligence and Cybercrime (IJCIC) aims to contribute to the growing field of cyber criminology and cyber security. The IJCIC is eager to work with scholars, policy analysts, practitioners, and others to enhance theory, methods, and practice within cybercrime and cyber security at the regional, national, and international levels.

Source: K. Choi., & C. S. Lee. (2018). *International Journal of Cybersecurity Intelligence and Cybercrime*, 1 (1), 1-4.

A policy paper by Katalin Parti, Tibor Kiss, and Gergely Koplányi—“Architecture of aggression in cyberspace: Testing cyber social deviance in youth utilizing the Bryant-Smith Aggression Scales” tested the online aggression-violence scale on a sample of young adults (aged 19-24) studying in law schools and social work bachelor of arts courses throughout Hungary. Parti and her colleagues found that cyberspace, online anonymity, and online social networking sites, do not work as a

catalyst of social violence. Their study emphasizes that while higher education has a significant role in establishing control, better teaching nonviolent communication, and coping strategies should be further developed. One way is to offer coordinated school-based anti-bullying programs across different disciplines.

Source: Parti, E., Kiss, T., & Koplányi, G. (2018). Architecture of aggression in cyberspace: Testing cyber social deviance in youth utilizing the Bryant-Smith Aggression Scales. International Journal of Cyber security Intelligence and Cybercrime, 1(1), 57-70

Dennis Giever presents a compelling argument for interdisciplinary programs in cyber security at the university level in his commentary—“An Argument for Interdisciplinary Programs in Cyber security”. We now live in a society where IT security and physical security do not have boundaries. He recommends that any security program take on a “all possible paths” or “balanced approach” to the protection of assets within an organization. Students in computer science, criminal justice, business, and human resources (among others), should learn and work collaboratively with other disciplines. A collaborative effort is also important to accomplish the myriad of tasks necessary to protect assets today.

Source: Giever, D. (2018). “An argument for interdisciplinary programs in cyber-security, International Journal of Cyber-security Intelligence and Cybercrime, 1(1), 71-76

This report in NIJ’s Research for Practice series describes the results of the Indiana and Florida telephone surveys and places these results in the context of other research to help managers determine what matters most in improving public satisfaction with police. This study also examined how satisfaction with police varied according to the demographic characteristics of respondents. Caucasians and nonblack minorities expressed significantly greater satisfaction with police than did their black neighbors. The research did not find gender differences in satisfaction with police. Differences between age groups were evident, however; respondents ages 18 to 32 reported significantly lower levels of satisfaction than did older persons. Homeowners expressed greater satisfaction than renters.

Source: John Ashcroft (2002), Satisfaction with Police—What Matters? U.S. Department of Justice Office of Justice Programs National Institute of Justice

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. This paper is an attempt to provide a glimpse on cyber-crime in India. This paper is based on various reports from news media and news portal.

Source: 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

This paper explores cyber-crime from different perspectives, providing a deeper analysis of the phenomena itself as more sophisticated technical tools have emerged. Making detection of such methods quite difficult for law enforcement authorities around the globe, since the rise of the deep-web has made the prevention of such crimes is difficult if not impossible. However, the main objective of this paper is to examine the effect of unemployment rates and GDP growth per capita on the level of cyber-attacks in 10 countries (USA, Belgium, the Netherlands, Japan, China, Italy, Spain, India, and Canada) during the period of 2005- 2017. In addition, this study seeks to provide insight into what might be the reason behind the fluctuating levels of attacks in these countries. This paper provides different authorities as well as the government with insight into how to take steps forward in preventing and combating these crimes.

Source: Al-Suwaidi et. al. – Estimating Causes of Cyber Crime: Evidence from Panel Data FGLS Estimator, International Journal of Cyber Criminology – ISSN: 0974 – 2891, July – December 2018. Vol. 12(2): 392–407

McGuire (2012) identified three main types (type I, II, and III) and six subtypes (swarm, hubs, extended hybrids, clustered hybrids, aggregates, and hierarchies) of cyber-organized crime groups and concluded that up to 80% of cyber-crime is organized crime. According to McGuire's report, certain key characteristics of traditional organized crime groups need to be reconsidered when groups are operating online. For instance, in cyberspace, the size of a group does not correlate with the impact and scope of their offenses, and many associations are highly transitory. The interpretation offered in the report is that cyberspace has augmented, rather than replaced, existing varieties of organized criminal organizations. To decide whether a certain network of offenders should be labeled organized crime, however, the report examined recurring offending patterns and the scale of activity,

they examined the debates around the definitions of organized crime, and they adopted the organized crime umbrella term to include a broad range of groups exhibiting some degree of organization.

Source: McGuire, M. (2012) organised crime in the digital age London, UK: John Grieve Centre for Policing and Security

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. This content also includes anything that is below the searchable Internet that is inherently hidden, harder to get to, or not readily visible. Thus, it is compared this content to mining through subterranean layers of the earth in terms of scale, volatility, and accessibility.

Source: Ciancaglini, V., Balduzzi, M., Goncharov, M., & McArdle, R. (2013). Deepweb and Cybercrime, Trend micro report

According to **Kshetri (2010)**, people in developing countries are attracted to cyber-crimes because of high unemployment rate and low wages; there are reports indicating that traditional organized crime groups in these countries have been involved in such attacks after diverting their operations to cyberspace to expand their illicit activity globally.

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

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

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

The Computer worms have drawn main attention in the research group of people due to their extremely undesirable influence on the local networks and also on

internet. to understand the adverse impacts posed by computer worms it is necessary to understand the classes of worms. This paper describes the definition of Computer worm, History and Time line of Computer worms, classification of Computer Worms based on scanning and also based on their behavior, life cycle of Computer worm

Source: B. Rajesh, Y.R. Janardhan Reddy, B. Dillip Kumar Reddy (2015), A Survey Paper on Malicious Computer Worms, International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015)

The purpose of this research was to examine if job satisfaction predicts job performance among police officers in Malaysia. Data was collected from 262 police officers who are currently working in the Royal Malaysia Police (RMP) located in Georgrtwon, Pulau Pinang, Malaysia. Participation in the research was voluntary. The results indicate that job satisfaction is positively correlated with performance. Supervision, co-workers, and work have a significantly positive impact on job performance, while the effect on pay and promotion is not significant. The findings of this study provide some insight to extend research in organizational behavior among police officers in North Earth Police Department, Pulau Pinang. In addition, studying the relationship between job satisfaction and job performance has synergistic and complementary effects on each of police officer attitudes that exceed the individual effects. Intervention to improve the police officers' job satisfaction should be kept developed in the future, especially to enhance the better performance in RMP. Implications, limitation, and suggestion for further research and practitioners are discussed in this study.

Kok Yeow Chong, Daisy Mui Hung Kee (2019), Job Satisfaction and performance of police officers in Penang, International Conference on Business Sustainability and Innovation, The European Proceedings of Social & Behavioural Sciences, EpSBS, ISSN: 2357-1330

This cross sectional survey seeks to profile the degree, spread or extent of various facets of job satisfaction against identified personal socio-demographic variables on a purposive sample of 687 police personnel hailing from 17 police stations in Mysore Urban District, Karnataka, India. The 36-item Likert Scale of Job Satisfaction Survey covering 9 facets revealed mean score of 129.85 (SD: 21.38;60.12%) which is interpreted as 'ambivalence' on the measuring instrument. This sense of uncertainty is reflected across socio-demographic variables except gender and number of

dependents although within the same expressed bandwidth of ambiguity ($p: <0.05$). A facet-wise and item analysis show highest source for job satisfaction emerge from their nature of work, supervision and camaraderie with co-workers, whereas the source of their dissatisfaction stem from non-availability of rewards, low salaries, poor perks, lack of promotions or benefits and wanting work conditions. The findings are presented and discussed in the light of a need to undertake job satisfaction research on a larger continual basis for updating and optimizing the available human resources in the police organization.

Source: L. Lokesh, Swati Patra & S. Venkatesan (2016), Job Satisfaction among Police Personnel: A Socio-Demographic Study

The paper has two purposes – first, to examine the dimensionality of police officer satisfaction and, second, to identify the impact of the groups of factors on police officer satisfaction. The measurement of satisfaction of all police officers in the Slovenian Police based on the comprehensive on-line questionnaire, Factor analysis was used to formulate the facets of satisfaction. Multiple linear regression analysis was performed to identify the predictors of three facets of police officer satisfaction. Three facets of police officer satisfaction were determined and the influence of three types of factors (demographic, job-related and organizational-support-related factors) on them was investigated. The results show that worst assessed facet was (1) salary and security, whereas no significant differences were found between two other facets, namely (2) relationships and leadership and (3) tasks and working conditions. The three factors influenced police officer satisfaction with different levels of intensity. The current economic situation in the state, especially in the public sector and in the police service, definitely impacts the results of the survey. The survey was conducted just before the announcement of savings measures in the Slovenian public sector. Since it was conducted online, we assume that for some police officers this probably meant that anonymity could not be assured. The survey was performed in order to identify the opportunities for improvements in police management. The results indicate the importance of leadership, communication and participation in the work of police officers, especially during a period of limited financial resources.

The far strongest influence on police officer satisfaction is that of the police officers' feeling that the police will support and protect them in case they are exposed while performing their legitimate and professional work. Trust in one's immediate superior

also has a strong influence. Both could be an important signal to the management of the police to focus on activities to increase cohesiveness within the police and constantly promote the feeling of belongingness to the police among all its members.

Source: Nina Tomažević, Janko Seljak, Aleksander Aristovnik (2015), Factors Influencing Police officer Satisfaction in the Police Service: The Case of Slovenia

The increasing expansion and diversification in the strategies and practices of cybercrime has become a difficult obstacle in order both to understand the extent of embedded risks and to define efficient policies of prevention for corporations, institutions and agencies. The present study represents the most comprehensive review of the origin, typologies and developments of Cybercrime phenomenon over the past decade so far. By means of this detailed study, this paper tackles the issue first describing and discussing former different criteria of classification in the field and secondly, providing a broad list of definitions and an analysis of the cybercrime practices. A conceptual taxonomy of cybercrime is introduced and described. The proposal of a classification criterion is used in conjunction with a cybercrime hierarchy derived from the degrees and scale of vulnerability and targets.

Source: Regner Sabillon, Jeimy Cano, Victor Cavaller, Jordi Serra (2016), Cybercrime and Cybercriminals: A Comprehensive Study, International Journal of Computer Networks and Communications Security VOL. 4, No. 6, June 2016, 165–176

Dissatisfied workers are at risk for negative occupational behaviors such as job turnover, poor performance, work avoidance, decreased morale among coworkers, and physical or legal liability. Relying heavily on demographic (e.g., sex, race, education) and occupational (e.g., rank, experience, assignment) explanatory factors, early empirical studies failed to effectively model the statistical correlates of police officer job satisfaction. Recent inquiries have found more success in explaining the variation in job satisfaction by examining a variety of work-related attitudes. The current study adds to this burgeoning area of research by assessing the role of internal and external dimensions of the work environment, as well as views of fairness and effectiveness, on the job satisfaction of police officers. Based on survey data from a midsized municipal police department in Florida, the multivariate analysis reveals a number of successful predictors of job satisfaction, especially for those officers with a street level assignment. A second analysis, based on qualitative coding of open-ended survey questions, finds differences in positive

and negative features of the occupation across varying levels of satisfied and dissatisfied respondents. Implications of these findings for police practitioners and researchers are discussed.

Source: Eugene A. Paoline III¹ and Jacinta M. Gau (2020), an Empirical Assessment of the Sources of Police Job Satisfaction, *Police Quarterly* 2020, Vol. 23(1) 55–81, the Author(s) 2019

In a more recent examination of the correlates of job satisfaction, Johnson (2012) surveyed 292 officers from 11 agencies in the Phoenix metro area. In addition to demographic characteristics, occupational features, and work related attitudes (job variety, job autonomy, job stress, role conflict, and cynicism), the author also assessed the relevance of the internal organizational climate (i.e., supervisor feedback, organizational support, and peer cohesion), finding that officers who reported more autonomy and peer cohesion were more satisfied with their jobs, while greater role conflict resulted in less satisfaction.

Johnson, R. R. (2012). Police officer job satisfaction: A multidimensional analysis. *Police Quarterly*, 15(2), 157–176

The internet has many uses for our life. It helps our work, and gives us some information that we need quickly. Along with the vigorous development of the internet, the development and the spread of malicious code which can harm our data and system in our computer are becoming even more unstoppable. To find out more the ins and the outs of computer worm, including how the work and how to overcome, it is necessary to study the classification of computer worm itself first. This paper presents taxonomy for classifying worm structure, worm attack, worm defense, and user defense. This paper presents the taxonomy for classifying computer worm into 4 main classifications, which are based on its structure, how they attack, how they defense itself from detection, and how user fight the computer worm

Source: Andhika Pratama and Fauzi Adi Rafrastara (2012), Computer Worm Classification, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 10, No.4, April 2012

2.2 THEORETICAL BACKGROUND OF THE STUDY

There are a lot of hacker categories; these categories include different terminology and iconography that create controversy over the computer attacker terms. The media and general public refer to people who are responsible for attacking and damaging computer systems as —hackersll. But using the term hacker to label a cybercriminal or computer vandal denigrates the term as well the historic concept. Most of hacker online activities are perfectly legal; the difference between hackers, hackers who commit crimes and cybercriminals rest upon their attitudes when a hacker accepts the activity and the motives.

Categories

The SANS Institute (2004) based on previous researcher's work have determined various categories and subgroups of hackers:

White hats: These individuals work within the laws of the hacker ethic (to do no harm) or as security experts.

Gray hats: This term was coined by L0pht – one of the best known old school hacking groups. These hackers are reformed Black Hats now working as security consultants.

Black Hats: These hackers are motivated by power, anger or hate. They do not have any qualms to steal or destroy network data that they penetrate.

Classes

These classes of hackers are under both Black Hat and White Hat categories:

Elite: They have the knowledge and skills of the highest level. This status can be gained by a particularly famous exploit, hack or longevity on the scene.

Script Kiddies: The most scorned subgroup within the larger hacker community. These tend to be the least skilled and youngest members using the tools created by elite hackers.

Cyber-terrorists: They use stenography and cryptology for exchanging information and sharing plots online. These hackers are considered to become the most serious of computer criminals.

Disgruntled (ex) police officers: one of the most dangerous, least publicized groups. These people believed they were owed special recognition for their corporate work and would take revenge for the lack of it.

Virus Writers: This group tends to exploit weaknesses found by hackers, then code methods to execute computer flaws.

Hacktivist: This name derives from combining the words activism and hacking. One of the fastest growing hacker subgroups, which are motivated to deface websites and launch Denial of Service (DOS) attacks to satisfy political, religious and social agendas

The EC-Council (2014) has created a different taxonomy based on Hacker classes. They highlight the differences between regular hacking versus ethical hacking. This categorization includes eight different classes:

Black Hats: Hackers with excellent computing skills that are attracted to malicious activities. Their motives are to cause damage, steal information, destroy data and earn money.

White Hats: Individuals with hacking skills those act to protect networks in a defensive way. They work in corporate environments as security analysts.

Gray Hats: Hackers that work both offensively and defensively at different situations.

Suicide Hackers: Hackers that aim to bring down critical infrastructure for radical causes and are not afraid to go to jail. They are related to suicide bombers and are active members of cyber terrorism groups.

Script Kiddies: The most unskilled hackers that are not well versed in hacking techniques. They tend to focus in getting high quantities of attacks rather than performing quality attacks.

Spy Hackers: These hackers are on contract to penetrate and gain trade secrets of their employer's competitors.

Cyber Terrorists: These could be people or organized groups that are motivated by political or religious motives to cause harm by disrupting large scale computer networks.

State Sponsored Hackers: State sponsored hackers that are employed to damage other countries networks and information systems.

Warren and Leitch (2009) have created an additional hacker category that was not considered before. The researchers have identified a sub group of hackers called —Hacker Taggers. These hackers like to deface websites with the intention of leaving a _hacker tag or _calling card behind. This tag or card is updated to show hacker's individual scores.

Definition of Computer Worm

Definition1: Computer worms are malicious software applications designed to spread via computer networks.

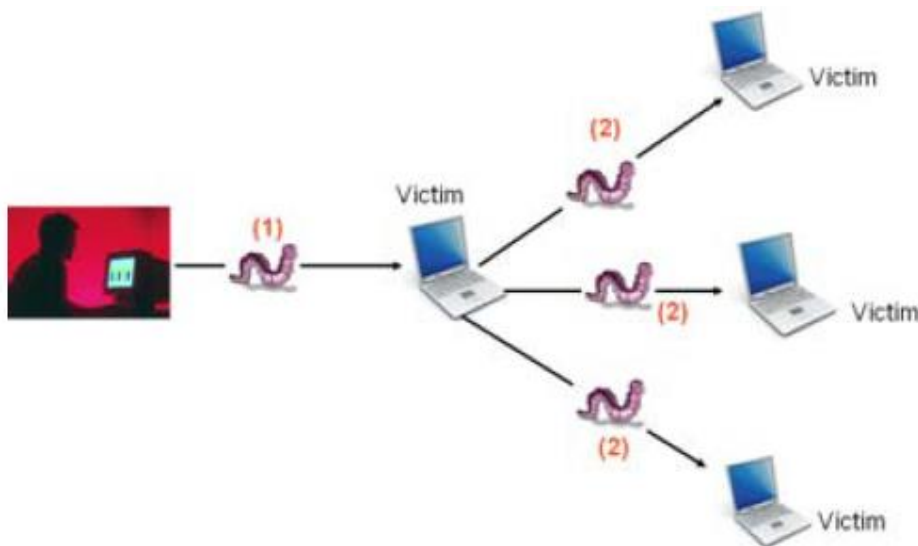
Definition2: A computer worm is a evil-intentioned program that can replicate and run itself. **Brief History of Computer Worm** The first ever program that could be called a Worm, as per definition, was developed for the assistance of air traffic controllers by Bob Thomas in 1971. This worm program would notify air traffic controllers when the controls of a plane moved from one computer to another. This worm named “creeper” would travel from one computer screen to another on the network showing the message “I am reaper! Catch me if you can! “The difference from most worms was that this creeper did not reproduce itself. The first Internet infection that required no human intervention to propagate was the Morris Worm, discovered in 1988 and released by Robert Morris. It spread very quickly, infecting a number of vulnerable computers in a matter of hours. The Morris Worm infected various machines and also used multiple exploits including buffer overflows, debugging routines in mail components, password sniffing, and other streams of execution to improve its ability to attack other computers. Although released on accident, the benign concept doesn’t really apply to the Morris Worm, as it had a significant amount of impact because of the bug in its code. When re infecting a computer, there remained the possibility that the new infection would be persistent, allowing other worms to run and terribly impact system performance. However, this caused the worm to be noticed instantly, and therefore, quickly contained.

Modern Worms: Active computer worms have returned to prominence in recent times. The first one to cause an eruption was Code Red. This infection proved how quickly a simple self-replicating program could spread via the internet’s current infrastructure. Code Red exploited a buffer flow condition in the Microsoft IIS (Internet Information Server). It was able to propagate quickly because of the “always on” nature of IIS and many versions of the Windows operating system. Code Red was also equipped with scanning capabilities that improved its throughput and gave it the ability to elude numerous IP address security features.

Life of Computer Worm

Once the worm enters in any one of the host computer, the life of the worm contain the following phases they are

- A. Scanning for a victim
- B. Exploiting the victim
- C. Payload
- D. Cloning itself onto the victim
- E. Stealth techniques used to hide it



Classification of Computer Worms

A. Classification based on behavior

- **Stealth worms:** This worm doesn't spread in a rapid fashion but instead they spread in a stealthy. They are very difficult to detect.
- **Polymorph worms:** To make the signature based detection more complicated these worms can change themselves during the propagation.
- **File worms:** These worms are modified version of viruses but unlike viruses this worms does not connect their presence with any executable files. They simply copy their code to some other disk or directory hoping that these new copies will someday be executed by the user.
- **Multi-vector worms:** This type of worms use different type of propagation methods in order to make more hosts vulnerable for attack and effectively propagate behind firewalls.

- **Email worms:** Email themselves to other email addresses and make the user execute email Attachments with malicious code or use bugs in the email programs to get attachments executed automatically.

B. Classification based on scanning

- **Random scanning:** Random Scanning worm will generate a random IP addresses using a pseudorandom number generator. Thus every host on the network is equally likely to be scanned. Code Red v2 and SQL Slammer are the random scanning worms.
- **Localized scanning:** Localized scanning is a simple technique used by computer worms to search for the vulnerable hosts. Localized scanning trades off between the local and the global search of vulnerable hosts and has been used by Code Red II and Nimda worms
- **Sequential scanning:** Sequential scanning worms' scans IP addresses sequentially. After the worm compromises a vulnerable host, it checks the host next to this vulnerable host. Blaster worm employed sequential scanning.
- **Topological scanning:** Topological scanning worms rely on the local information contained in the compromised hosts to locate new targets. Local information includes etc. hosts file, email addresses etc. Topological scanning was used by Morris worm.
- **Hit list scanning:** The worm writer gathers a list of potentially vulnerable hosts beforehand, which are targeted first when the worm is released. This speeds up the spread of the worm at an initial stage. Hit list scanning was used by Slammer worm.

CHAPTER 3

RESEARCH METHODOLOGY

Research methodology is a way of systematically solving the research problem. Research methodology deals with the research design used and methods used to present the study.

3.1 TYPE OF PROJECT

A research design is a detailed blue print used to guide a research study toward its objective. The process of designing a research study involves many interrelated decisions. The most significant decision is the choice of research approach, because it determines how the information will be obtained. The choice of the research approach depends on the nature of the research that one wants to do. The research design adopted for this study is Exploratory Research. Exploratory method was adopted because it deals with description of the state of affairs as it exists at present. The wellness of police officers is a retention measure for any organisation and it is a non-exception to this industry also. Personal interviews and observation methods are used to collect primary data. A questionnaire is designed to measure the satisfaction level of police officers working for cyber-crime department with regard to their wellness measures. A research design is the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy in procedure. It is the conceptual procedure with in which research is conducted.

3.2 SOURCES OF DATA

For the purpose of the study, both primary and secondary data has been obtained from officers of police department and with the help of the published information provided by the police officers working for cyber-crime department

Primary data is collected by issuing a well-designed questionnaire to the officers and their opinions and suggestions were sought with the help of the questionnaire.

Secondary data is gathered with the help of the literature that has been obtained from the department in the various forms as such magazines, journals, annual report and additional information.

Apart from the questionnaire I took the help of secondary data sources as:

- ✚ Records and documents
- ✚ Magazines and other brochures published
- ✚ Newspapers and other data sources
- ✚ Websites.

3.3 SAMPLING DESIGN

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

Sample Size: 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: Area of survey is Chennai

3.4 TOOLS & TECHNIQUES

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.

- ✚ Percentage method
- ✚ Chi-square analysis
- ✚ Correlation
- ✚ Regression
- ✚ Anova

3.5 LIMITATIONS OF THE STUDY

- The study is restricted to Cyber-crime officers alone.
- Due to time constraint the sample size is restricted.
- The study considered only 145 samples.
- The officers could not contribute more time. Some of them are not willing to answer
- The research may not reveal exact results due to the bias answers of the officers

CHAPTER 4

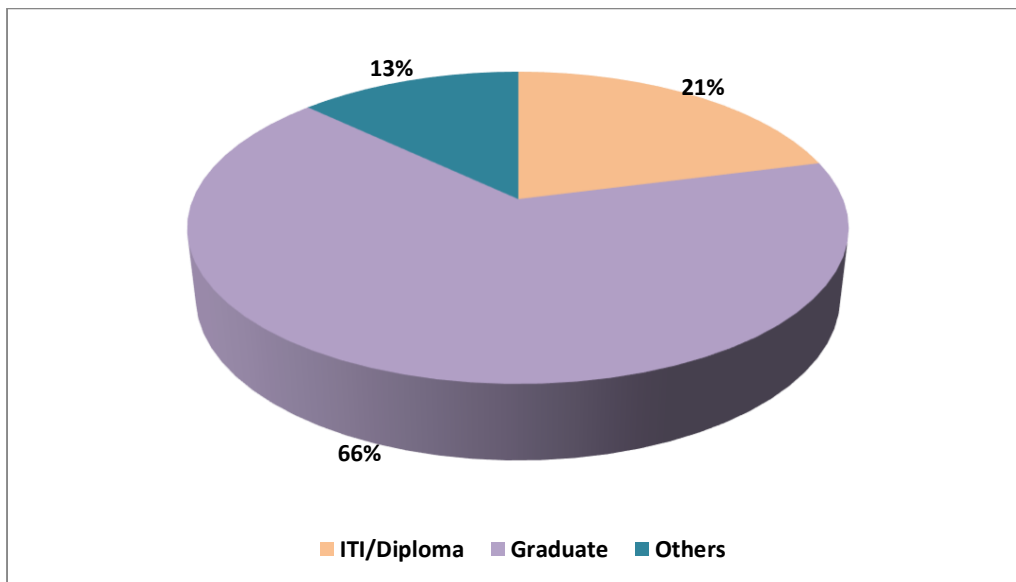
DATA ANALYSIS & INTERPRETATION

4.1 DESCRIPTIVE ANALYSIS – PERCENTAGE METHOD

TABLE 4.1.1: EDUCATIONAL QUALIFICATION OF THE RESPONDENTS

Frequency	No. of Respondents	Percentage (%)
ITI/Diploma	31	21%
Graduate	95	66%
Others	19	13%
Total	145	100.0%

CHART 4.1.1: EDUCATIONAL QUALIFICATION OF THE RESPONDENTS

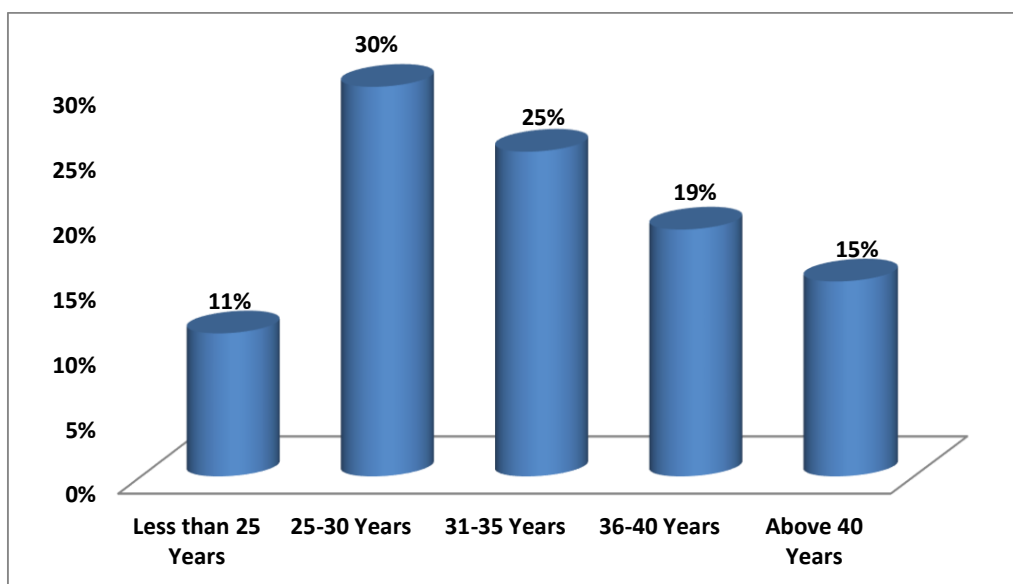


Interpretation: 21% respondents are ITI / diploma holders, 66% of them are graduates, and 13% of the respondents are having other qualifications

TABLE 4.1.2: AGE OF THE RESPONDENTS

Frequency	No.of Respondents	Percentage
Less than 25 Years	16	11%
25-30 Years	44	30%
31-35 Years	36	25%
36-40 Years	27	19%
Above 40 Years	22	15%
Total	145	100.0%

CHART 4.1.2: AGE OF THE RESPONDENTS

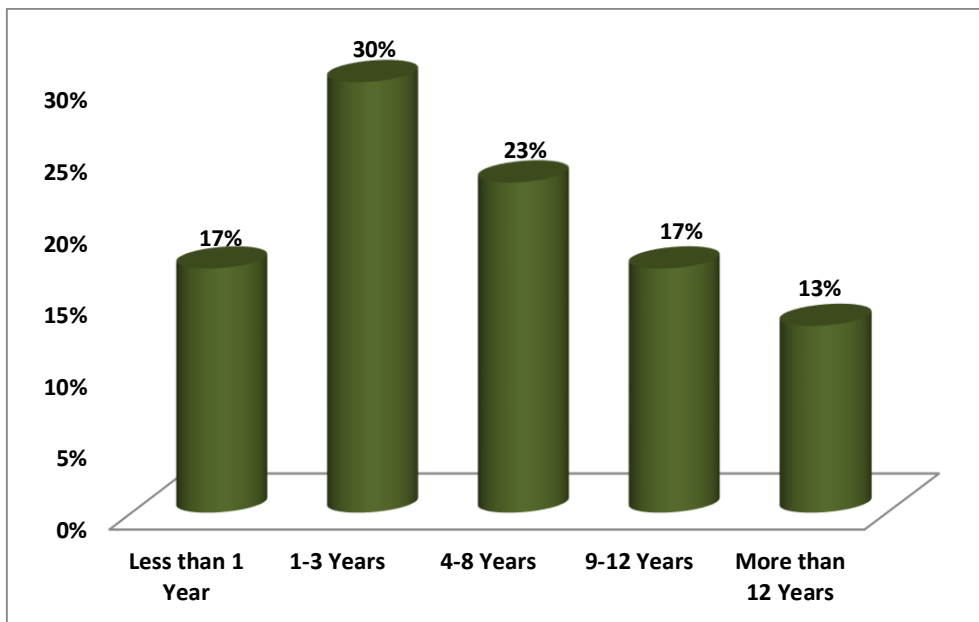


Interpretation: 11% respondents are having less than 25 years of experience, 30% of them 25-30 years old, 25% of them are 31-35 years old, and 19% of the respondents are 36-40 Years old and rest 15% of them are more than 40 years old

TABLE 4.1.3: WORK EXPERIENCE OF THE RESPONDENTS

Frequency	No.of Respondents	Percentage
Less than 1 Year	24	17%
1-3 Years	43	30%
4-8 Years	34	23%
9-12 Years	25	17%
More than 12 Years	19	13%
Total	145	100.0%

CHART 4.1.3: WORK EXPERIENCE OF THE RESPONDENTS

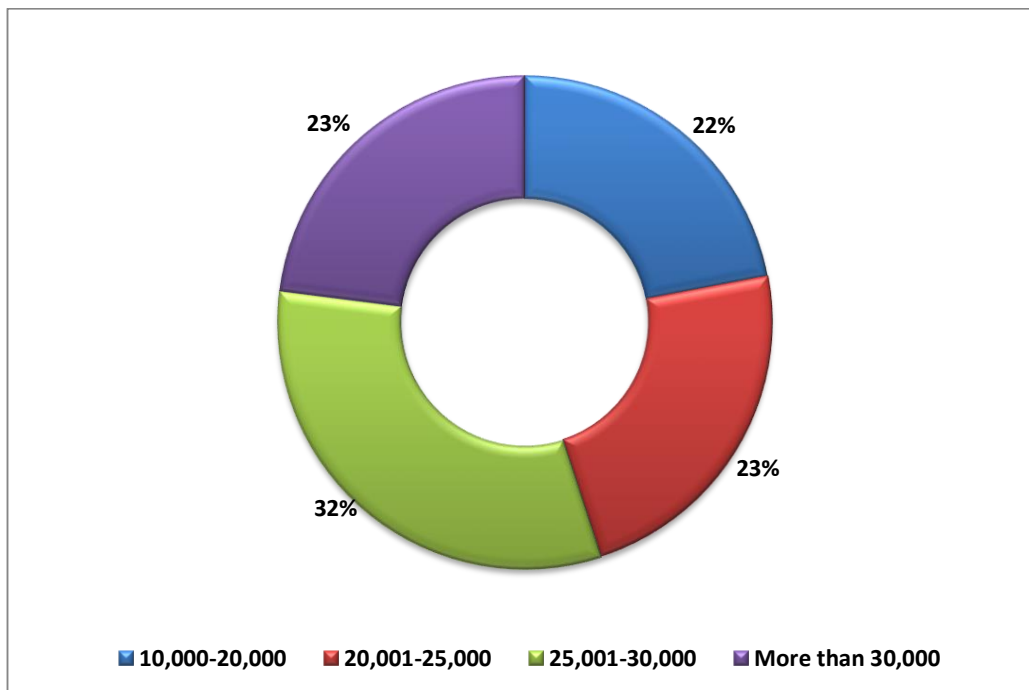


Interpretation: 17% respondents have less than 1 year experience, 29% of them have 1-3 years of experience, 23% of them have 4-8 years of experience, 17% respondents have 9-12 years of experience and rest 13% have more than 12 years of experience

TABLE 4.1.4: INCOME LEVEL OF THE RESPONDENTS

Frequency	No.of Respondents	Percentage
10,000-20,000	32	22%
20,001-25,000	34	23%
25,001-30,000	46	32%
More than 30,000	33	23%
Total	145	100.0%

CHART 4.1.4: INCOME LEVEL OF THE RESPONDENTS

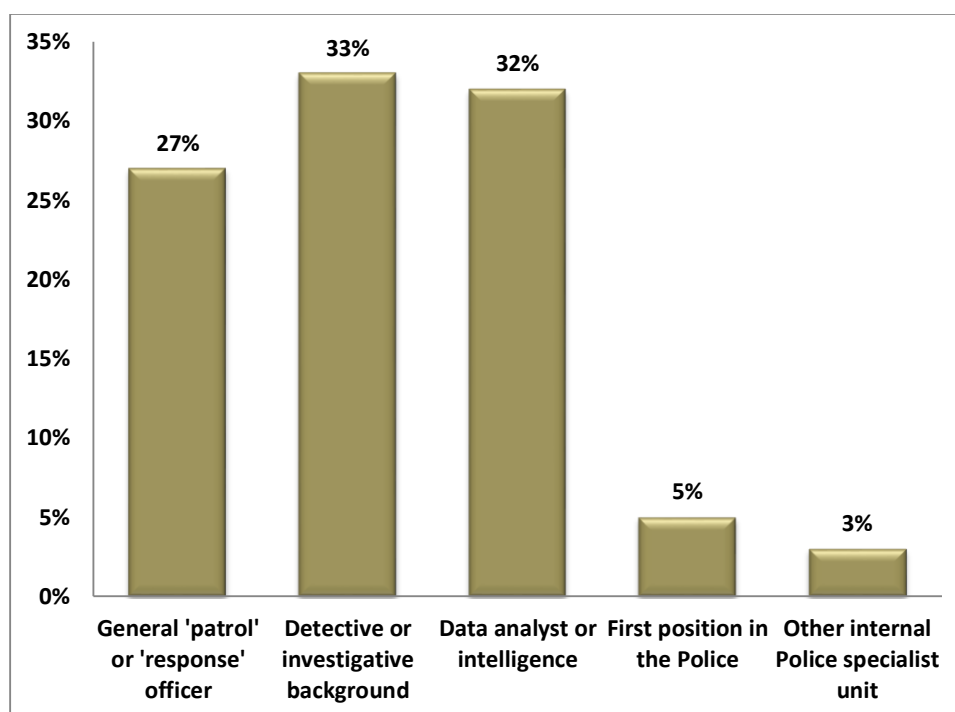


Interpretation: 22% respondents are earning 10,000-20,000 per month, 23% respondents' income per month is 20,001-25,000, 32% of them are earning 25,001-30,000 per month, 23% respondents are earning more than 30,000 per month

**TABLE 4.1.5: ROLE IMMEDIATELY PRIOR TO JOINING THE CYBER- CRIME
UNIT**

Frequency	No.of Respondents	Percentage
General 'patrol' or 'response' officer	39	27%
Detective or investigative background	48	33%
Data analyst or intelligence	46	32%
First position in the Police	7	5%
Other internal Police specialist unit	5	3%
Total	145	100.0%

**CHART 4.1.5: ROLE IMMEDIATELY PRIOR TO JOINING THE CYBER- CRIME
UNIT**

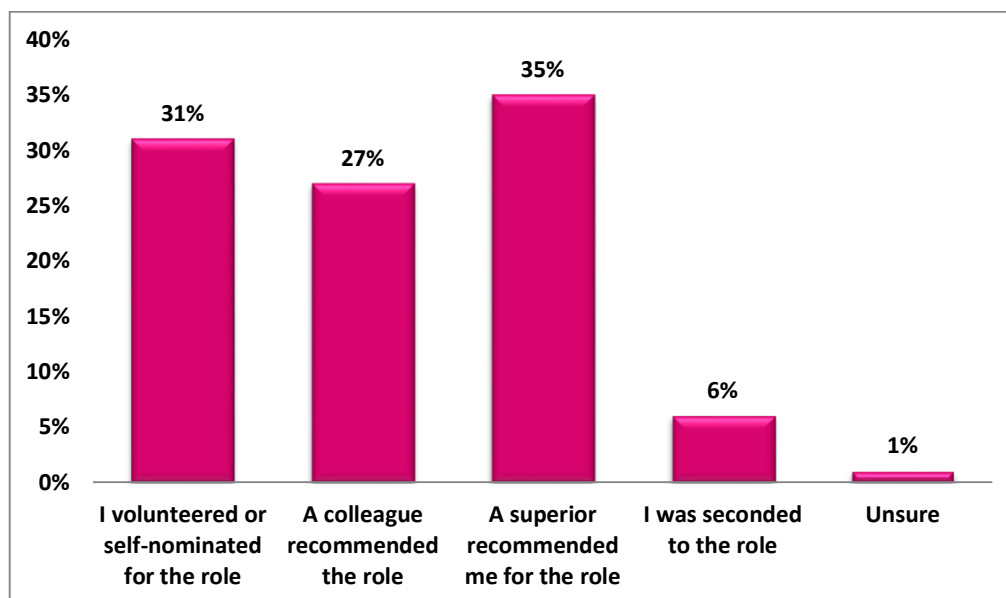


Interpretation: 27% respondents said their role immediately before joining the cyber-crime unit was General 'patrol' or 'response' officer, 33% of them said they were in the detective or investigative background with this, 32% of the respondents were in data analyst or intelligence unit, 5% respondents were working as a police and rest 3% of them were working on other internal Police specialist unit.

**TABLE 4.1.6: CIRCUMSTANCE THROUGH THEY JOINED THE CYBER-CRIME
UNIT**

Frequency	No.of Respondents	Percentage
I volunteered or self-nominated for the role	45	31%
A colleague recommended the role	39	27%
A superior recommended me for the role	51	35%
I was seconded to the role	8	6%
Unsure	2	1%
Total	145	100.0%

**TABLE 4.1.6: CIRCUMSTANCE THROUGH THEY JOINED THE CYBER-CRIME
UNIT**

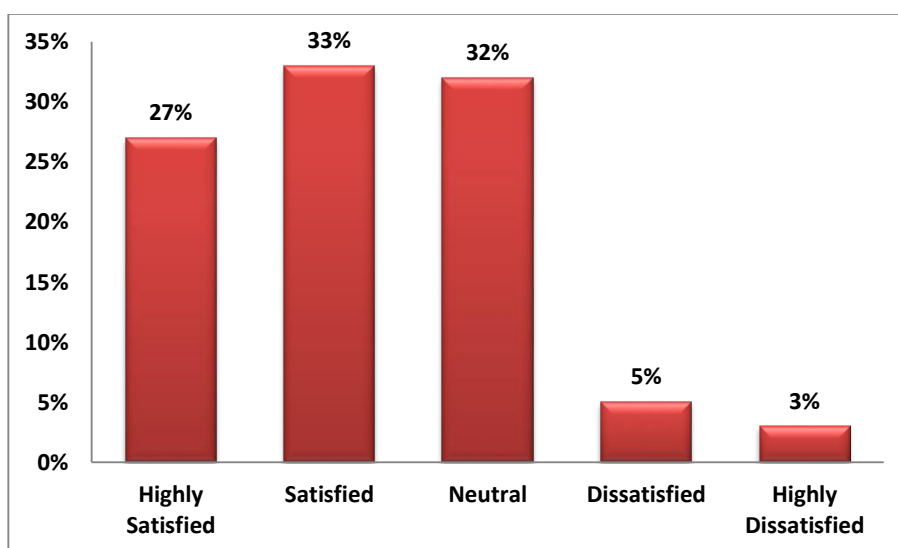


Interpretation: 31% respondents volunteered or self-nominated themselves for their present role, 27% of them said their colleague recommended for that role, 35% of the respondents said they were recommended by their superior for this role, 6% respondent said they were seconded for that role and rest 1% of them said they were unsure about that

TABLE 7: COMFORTABLE WITH THE WORKING HOURS

Frequency	No.of Respondents	Percentage
Highly Satisfied	39	27%
Satisfied	48	33%
Neutral	46	32%
Dissatisfied	7	5%
Highly Dissatisfied	5	3%
Total	145	100.0%

CHART 4.1.7: COMFORTABLE WITH THE WORKING HOURS

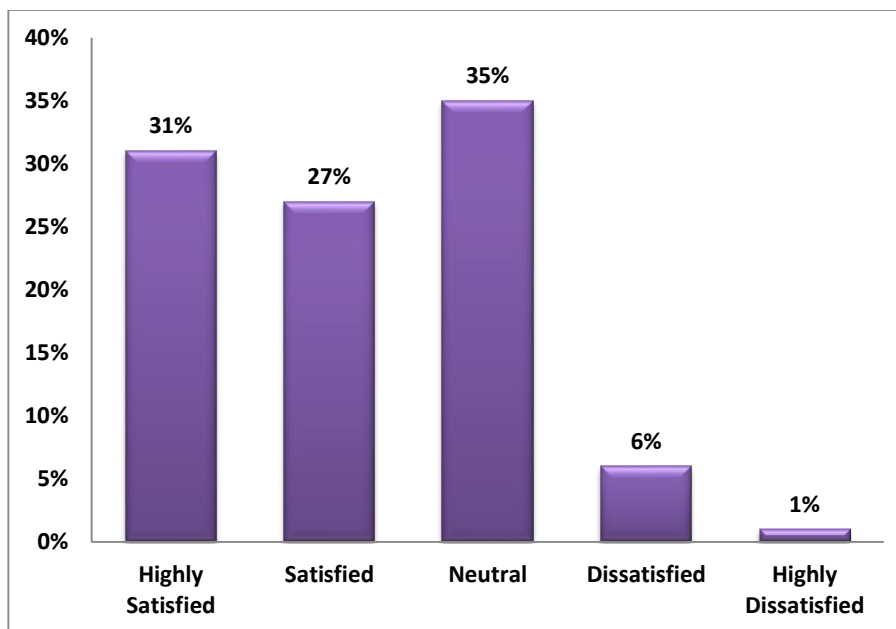


Interpretation: 27% respondents are highly dissatisfied with the comfortable working hours, 33% of them are dissatisfied with this, 32% of the respondents are neutral towards this, 5% respondent are found to be satisfied and rest 3% of them are highly satisfied.

TABLE 4.1.8: JOB IS INTERESTING AND PROSPECTIVE

Frequency	No.of Respondents	Percentage
Highly Satisfied	45	31%
Satisfied	39	27%
Neutral	51	35%
Dissatisfied	8	6%
Highly Dissatisfied	2	1%
Total	145	100.0%

TABLE 4.1.8: JOB IS INTERESTING AND PROSPECTIVE

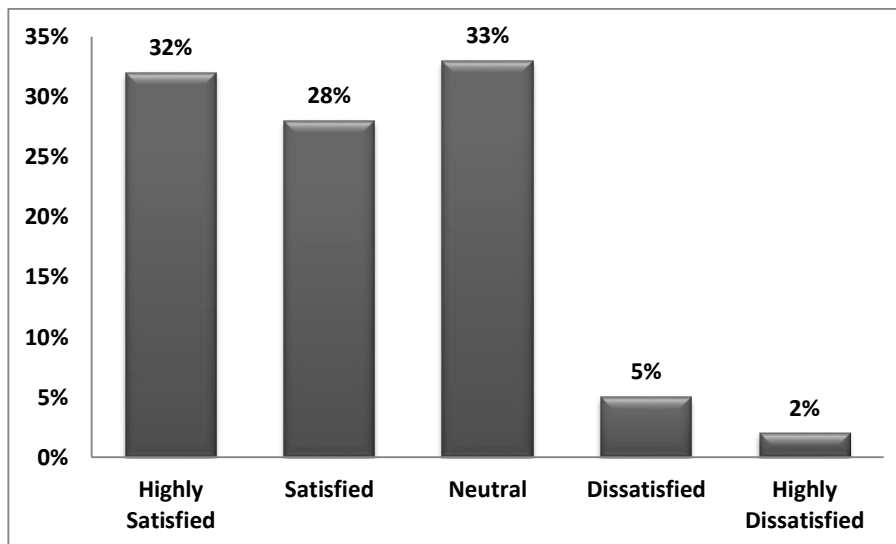


Interpretation: 31% respondents are highly dissatisfied with the prospective and interesting job, 27% of them are dissatisfied with this, 35% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.

**TABLE 4.1.9: FEELING PROUD TO BE A PART OF CYBER-CRIME
DEPARTMENT**

Frequency	No.of Respondents	Percentage
Highly Satisfied	46	32%
Satisfied	41	28%
Neutral	48	33%
Dissatisfied	7	5%
Highly Dissatisfied	3	2%
Total	145	100.0%

**CHART 4.1.9: FEELING PROUD TO BE A PART OF CYBER-CRIME
DEPARTMENT**

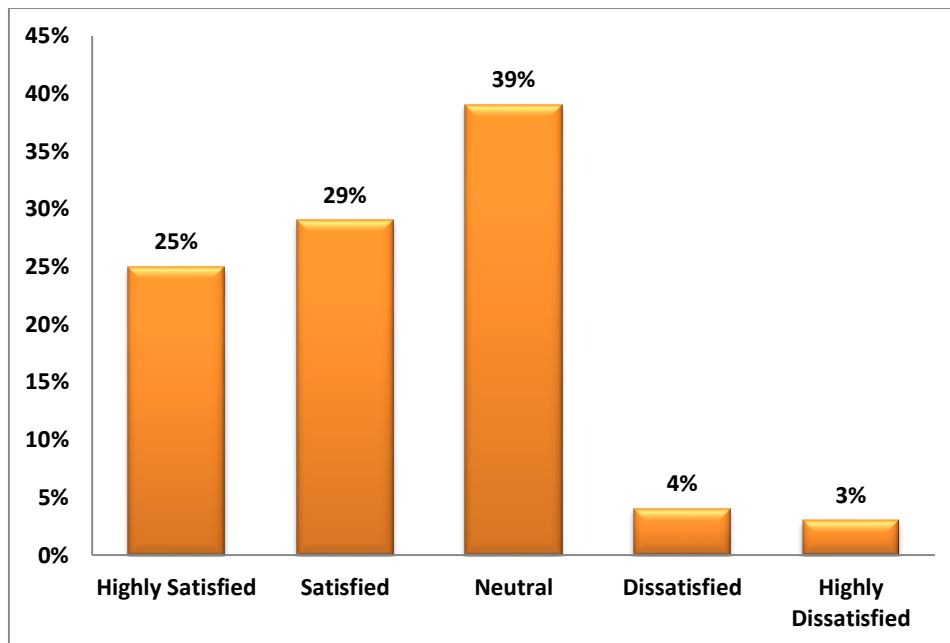


Interpretation: 32% respondents are highly dissatisfied with the part of the cybercrime department, 28% of them are dissatisfied with this, 33% of the respondents are neutral towards this, 5% respondent are found to be satisfied and rest 2% of them are highly satisfied.

TABLE 4.1.10: SATISFACTION WITH THE WORK HOURS AND SHIFTS

Frequency	No.of Respondents	Percentage
Highly Satisfied	37	25%
Satisfied	42	29%
Neutral	56	39%
Dissatisfied	6	4%
Highly Dissatisfied	4	3%
Total	145	100.0%

CHART 4.1.10: SATISFACTION WITH THE WORK HOURS AND SHIFTS

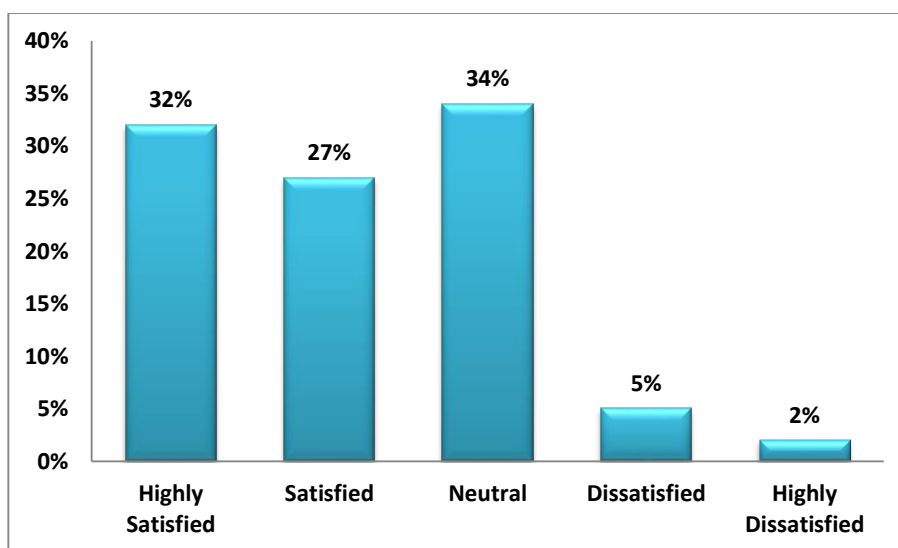


Interpretation: 25% respondents are highly dissatisfied with the working hours and working shift, 29% of them are dissatisfied with this, 39% of the respondents are neutral towards this, 4% respondent are found to be satisfied and rest 3% of them are highly satisfied.

TABLE 4.1.11: JOB IS AFFECTING THE HEALTH

Frequency	No.of Respondents	Percentage
Highly Satisfied	46	32%
Satisfied	40	27%
Neutral	49	34%
Dissatisfied	7	5%
Highly Dissatisfied	3	2%
Total	145	100.0%

CHART 4.1.11: JOB IS AFFECTING THE HEALTH

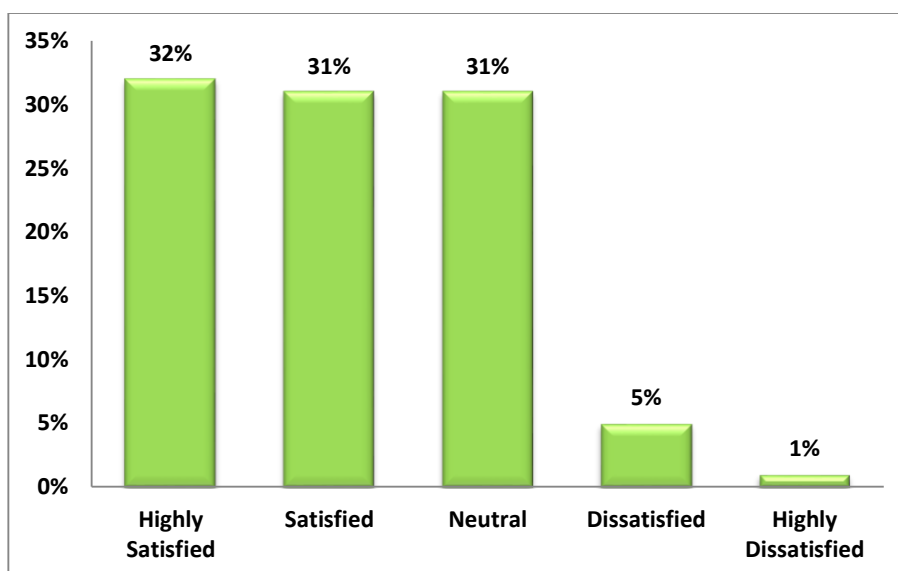


Interpretation: 32% respondents are highly dissatisfied with the job that is affecting their health, 27% of them are dissatisfied with this, 34% of the respondents are neutral towards this, 5% respondent are found to be satisfied and rest 2% of them are highly satisfied.

TABLE 4.1.12: PHYSICAL WORKING CONDITIONS

Frequency	No.of Respondents	Percentage
Highly Satisfied	46	32%
Satisfied	44	31%
Neutral	45	31%
Dissatisfied	8	5%
Highly Dissatisfied	2	1%
Total	145	100.0%

CHART 4.1.12: PHYSICAL WORKING CONDITIONS

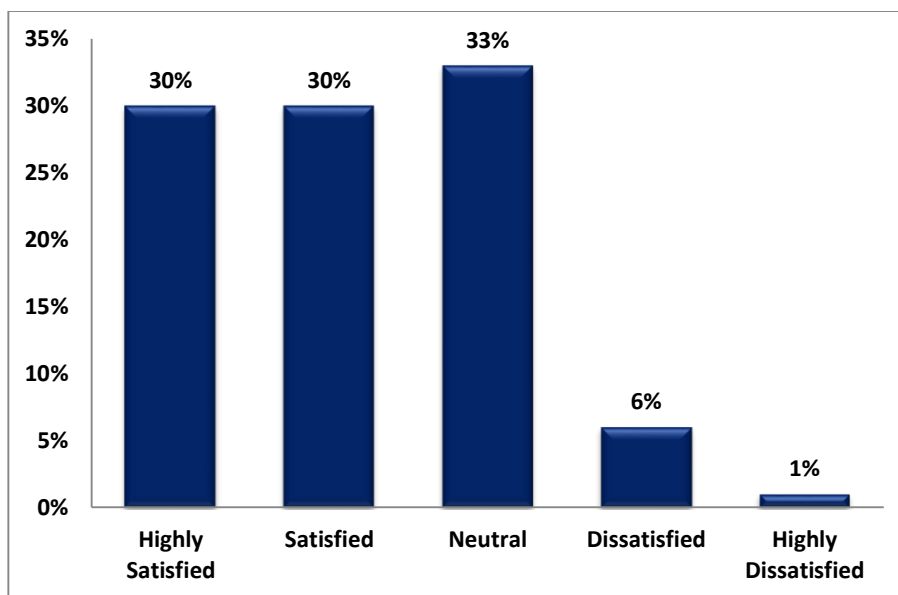


Interpretation: 32% respondents are highly dissatisfied with the physical working conditions of the department like Light, A/C, air etc, 31% of them are dissatisfied with this, 31% of the respondents are neutral towards this, 5% respondent are found to be satisfied and rest 1% of them are highly satisfied

TABLE 4.1.13: WORK PLACE IS LESS CROWDED AND CLEAN

Frequency	No.of Respondents	Percentage
Highly Satisfied	43	30%
Satisfied	44	30%
Neutral	48	33%
Dissatisfied	8	6%
Highly Dissatisfied	2	1%
Total	145	100.0%

CHART 4.1.13: WORK PLACE IS LESS CROWDED AND CLEAN

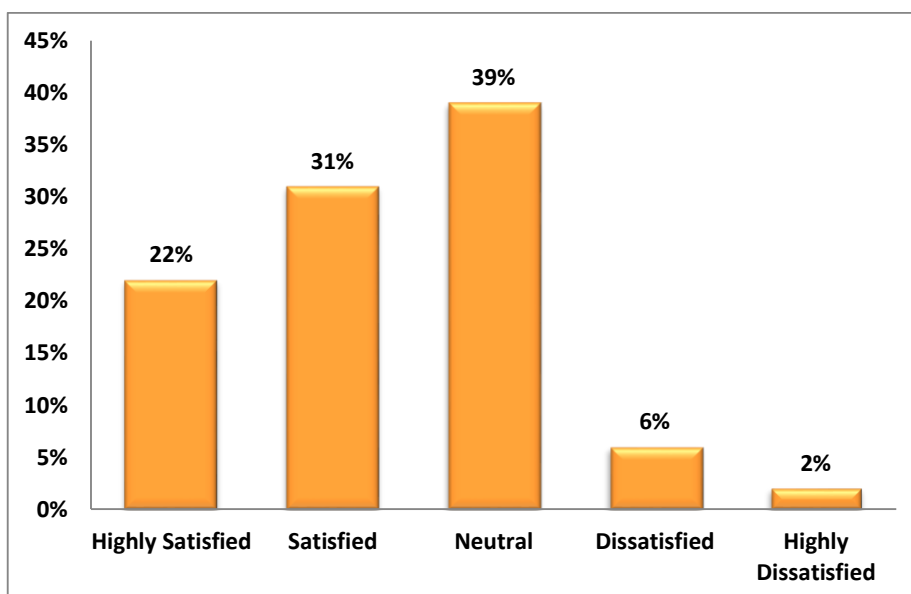


Interpretation: 30% respondents are highly dissatisfied with the less crowded and clean workplace, 30% of them are dissatisfied with this, 33% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied

TABLE 4.1.14: WORK ENVIRONMENT GIVES LESS EMPHASIS ON EQUIPMENT

Frequency	No.of Respondents	Percentage
Highly Satisfied	32	22%
Satisfied	45	31%
Neutral	57	39%
Dissatisfied	8	6%
Highly Dissatisfied	3	2%
Total	145	100.0%

CHART 4.1.14: WORK ENVIRONMENT GIVES LESS EMPHASIS ON EQUIPMENT

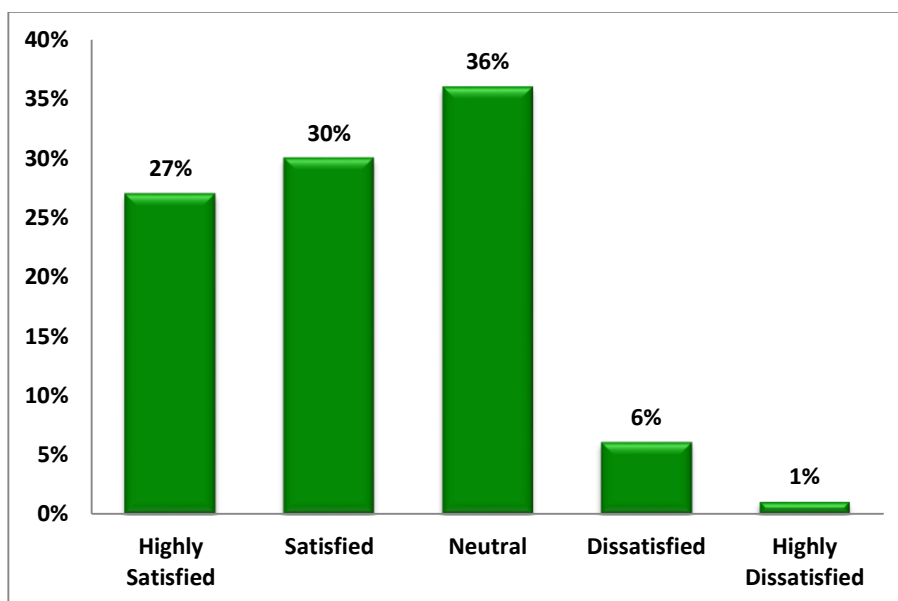


Interpretation: 22% respondents are highly dissatisfied with the workplace giving less emphasis on the equipment than the individual, 31% of them are dissatisfied with this, 39% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 2% of them are highly satisfied.

TABLE 4.1.15: ENVIRONMENT IS MORE ADAPTABLE AND COMFORTABLE

Frequency	No.of Respondents	Percentage
Highly Satisfied	39	27%
Satisfied	44	30%
Neutral	52	36%
Dissatisfied	8	6%
Highly Dissatisfied	2	1%
Total	145	100.0%

CHART 4.1.15: ENVIRONMENT IS MORE ADAPTABLE AND COMFORTABLE

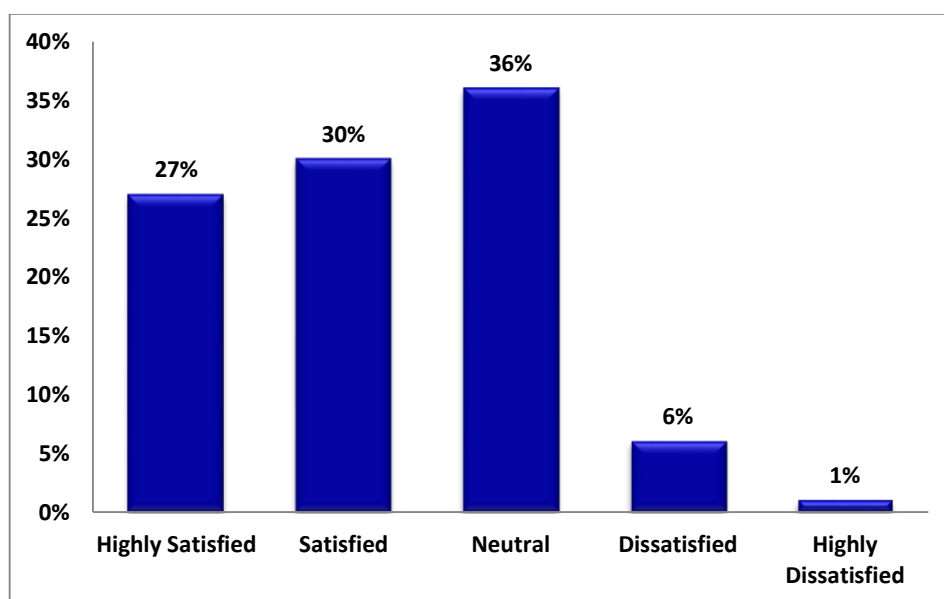


Interpretation: 27% respondents are highly dissatisfied with the adaptable and comfortable workplace, 30% of them are dissatisfied with this, 36% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.

TABLE 4.1.16: HEALTH IS NOT NEGLECTED DUE TO JOB

Frequency	No.of Respondents	Percentage
Highly Satisfied	38	27%
Satisfied	41	30%
Neutral	56	36%
Dissatisfied	8	6%
Highly Dissatisfied	2	1%
Total	145	100.0%

CHART 4.1.16: HEALTH IS NOT NEGLECTED DUE TO JOB

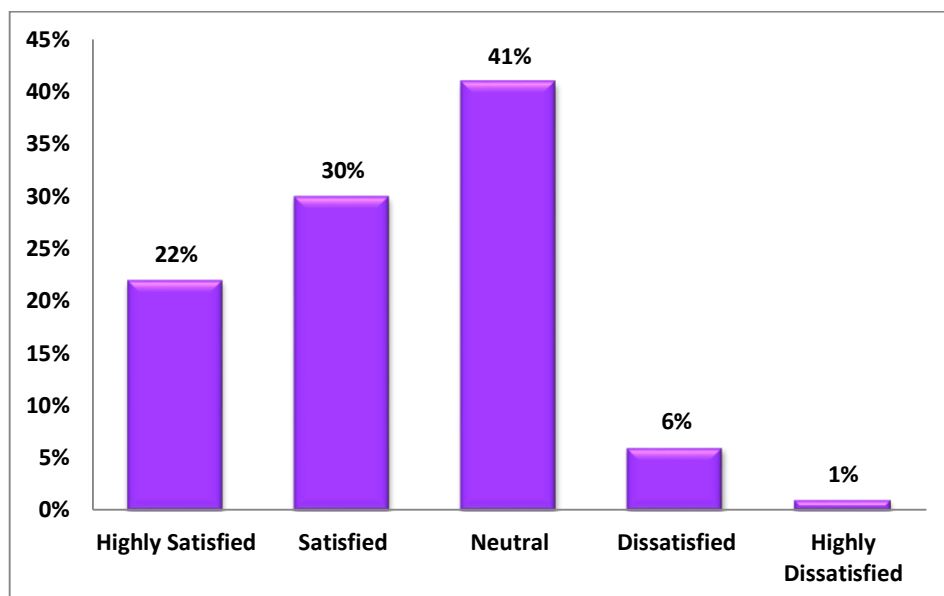


Interpretation: 27% respondents are highly dissatisfied with the fact that they do not neglect their health due to job, 30% of them are dissatisfied with this, 36% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.

TABLE 4.1.17: TIME AND ENERGY SPENT ON JOB WON'T AFFECT HEALTH ADVERSELY

Frequency	No.of Respondents	Percentage
Highly Satisfied	32	22%
Satisfied	43	30%
Neutral	60	41%
Dissatisfied	8	6%
Highly Dissatisfied	2	1%
Total	145	100.0%

CHART 4.1.17: TIME AND ENERGY SPENT ON JOB WON'T AFFECT HEALTH ADVERSELY

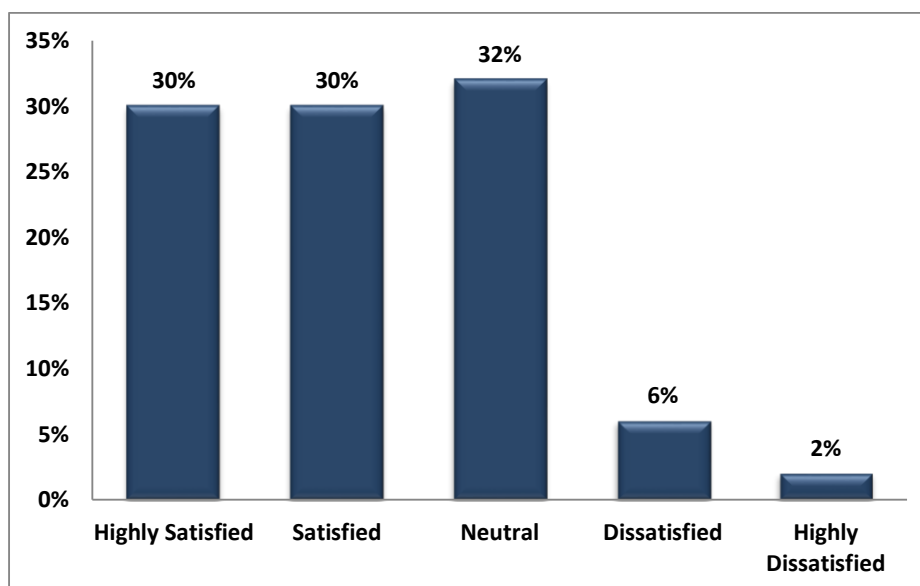


Interpretation: 22% respondents are highly dissatisfied with the energy and time that the officers spend on the job does not affect their life adversely, 30% of them are dissatisfied with this, 41% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.

**TABLE 4.1.18: NECESSARY SAFETY EQUIPMENTS ARE PROVIDED BY THE
CYBERCRIME DEPARTMENT**

Frequency	No.of Respondents	Percentage
Highly Satisfied	43	30%
Satisfied	44	30%
Neutral	47	32%
Dissatisfied	8	6%
Highly Dissatisfied	3	2%
Total	145	100.0%

**CHART 4.1.18: NECESSARY SAFETY EQUIPMENTS ARE PROVIDED BY THE
CYBERCRIME DEPARTMENT**

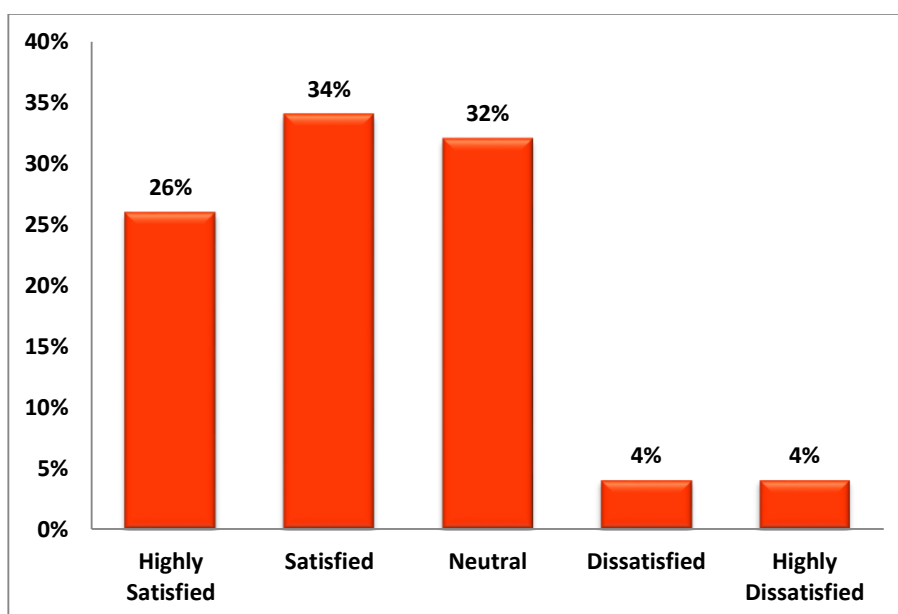


Interpretation: 30% respondents are highly dissatisfied with the necessary safety equipment provided by the cyber-crime department, 30% of them are dissatisfied with this, 32% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 2% of them are highly satisfied.

TABLE 19: SATISFACTION WITH THE DEPARTMENT'S WELFARE POLICIES

Frequency	No.of Respondents	Percentage
Highly Satisfied	38	26%
Satisfied	49	34%
Neutral	47	32%
Dissatisfied	6	4%
Highly Dissatisfied	5	4%
Total	145	100.0%

CHART 4.1.19: SATISFACTION WITH THE DEPARTMENT'S WELFARE POLICIES

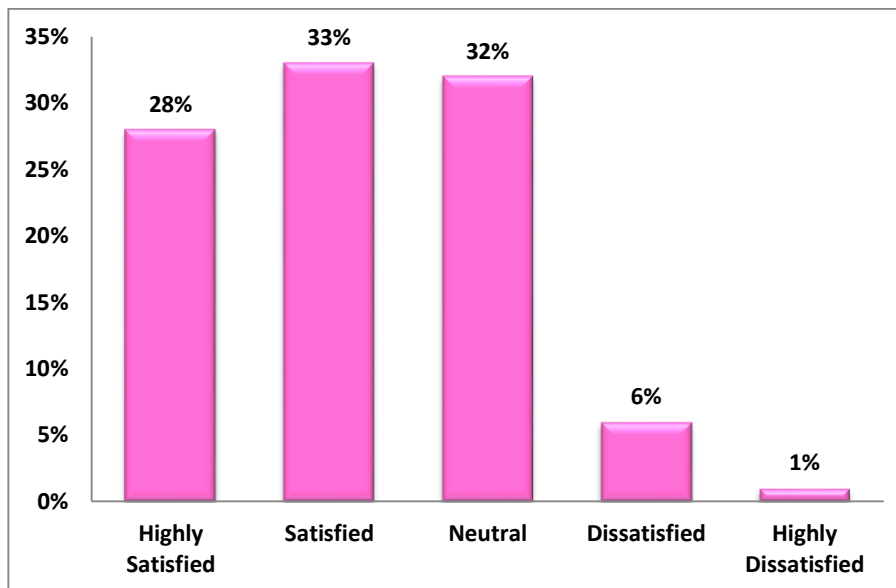


Interpretation: 26% respondents are highly dissatisfied with the department's welfare policies, 34% of them are dissatisfied with this, 32% of the respondents are neutral towards this, 4% respondent are found to be satisfied and rest 4% of them are highly satisfied.

TABLE 4.1. 20: COMPENSATION EARNED HELPS TO MAINTAIN SOCIALLY DESIRABLE STANDARD OF LIVING

Frequency	No.of Respondents	Percentage
Highly Satisfied	40	28%
Satisfied	48	33%
Neutral	47	32%
Dissatisfied	8	6%
Highly Dissatisfied	2	1%
Total	145	100.0%

CHART 4.1.20: COMPENSATION EARNED HELPS TO MAINTAIN SOCIALLY DESIRABLE STANDARD OF LIVING

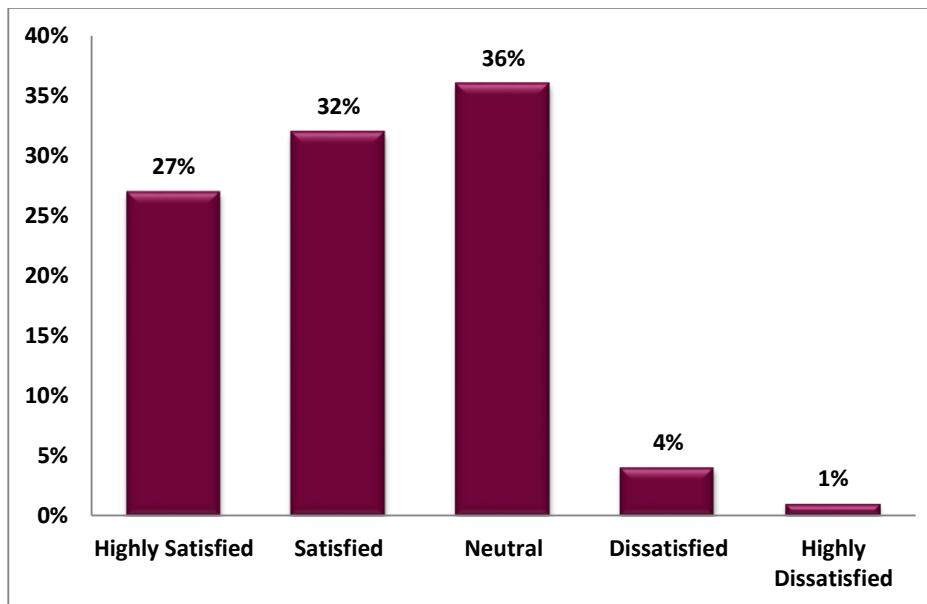


Interpretation: 28% respondents are highly dissatisfied with the compensation provided by the cyber-crime department help them to maintain a socially desirable standard of living, 33% of them are dissatisfied with this, 32% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.

**TABLE 4.1.21: SATISFACTION WITH REWARD SYSTEM OF CYBER-CRIME
DEPARTMENT**

Frequency	No.of Respondents	Percentage
Highly Satisfied	39	27%
Satisfied	47	32%
Neutral	52	36%
Dissatisfied	5	4%
Highly Dissatisfied	2	1%
Total	145	100.0%

**CHART 4.1.21: SATISFACTION WITH REWARD SYSTEM OF CYBER-CRIME
DEPARTMENT**

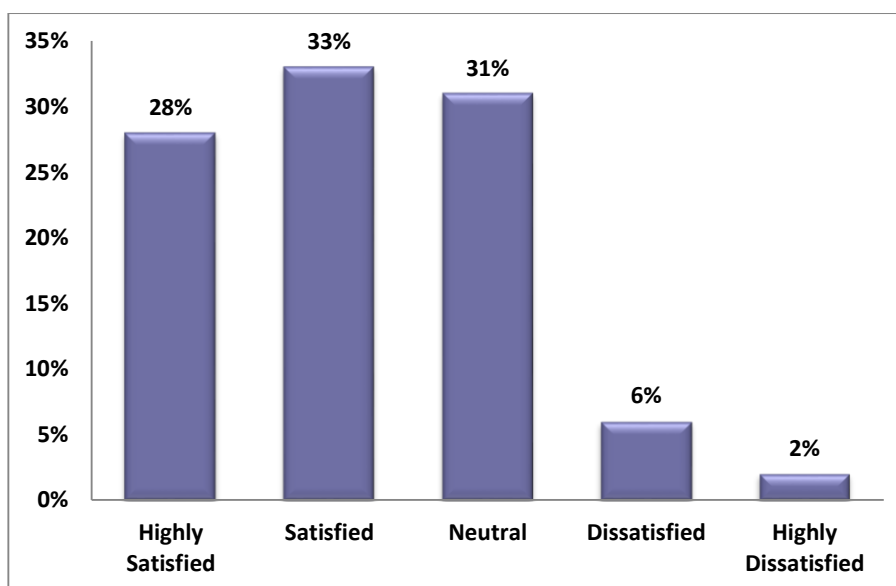


Interpretation: 27% respondents are highly dissatisfied with the rewards system their cyber-crime department, 32% of them are dissatisfied with this, 36% of the respondents are neutral towards this, 4% respondent are found to be satisfied and rest 1% of them are highly satisfied.

TABLE 4.1.22: CO-OPERATION WITH CO-OFFICERS

Frequency	No.of Respondents	Percentage
Highly Satisfied	41	28%
Satisfied	47	33%
Neutral	45	31%
Dissatisfied	9	6%
Highly Dissatisfied	3	2%
Total	145	100.0%

CHART 4.1.22: CO-OPERATION WITH CO-OFFICERS

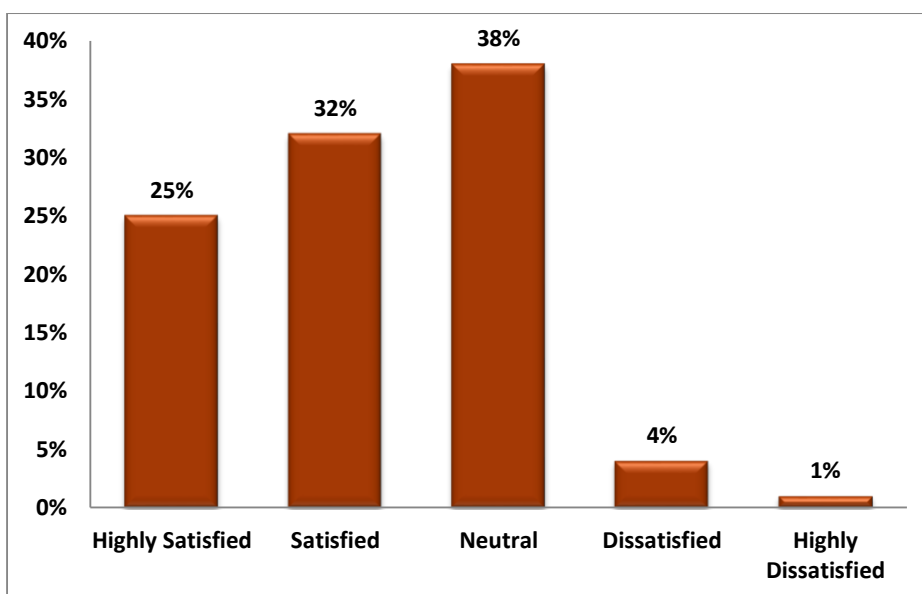


Interpretation: 28% respondents are highly dissatisfied with the co-operation within the co-workers, 33% of them are dissatisfied with this, 31% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 2% of them are highly satisfied.

TABLE 4.1.23: WORKING AS A TEAM IS NOT A PROBLEM

Frequency	No.of Respondents	Percentage
Highly Satisfied	36	25%
Satisfied	46	32%
Neutral	55	38%
Dissatisfied	6	4%
Highly Dissatisfied	2	1%
Total	145	100.0%

CHART 4.1.23: WORKING AS TEAM IS NOT A PROBLEM

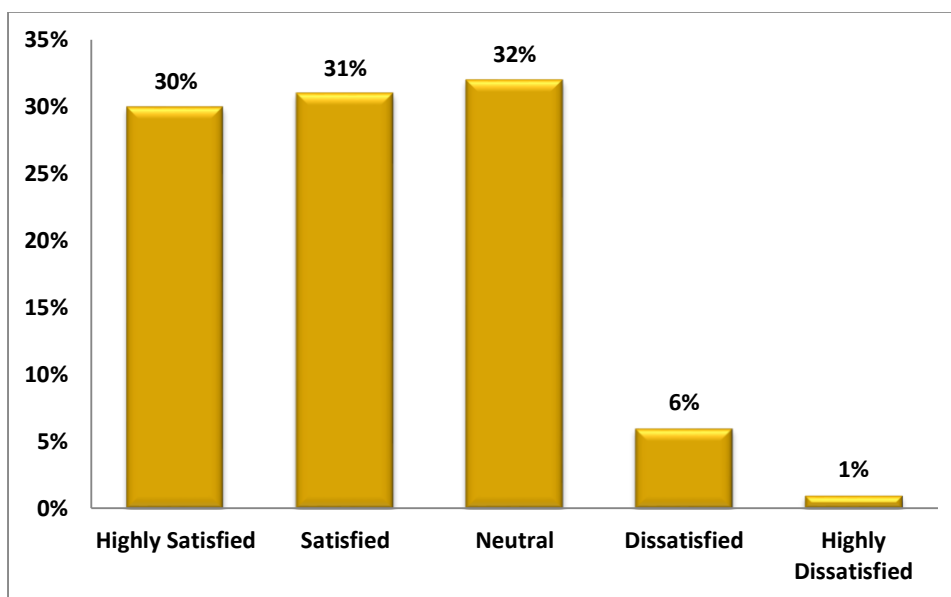


Interpretation: 25% respondents are highly dissatisfied with the working as a team in the department, 32% of them are dissatisfied with this, 38% of the respondents are neutral towards this, 4% respondent are found to be satisfied and rest 1% of them are highly satisfied.

TABLE 4.1.24: OFFICERS' INTERACT IN TERMS OF IDEAS AND FEELINGS

Frequency	No.of Respondents	Percentage
Highly Satisfied	43	30%
Satisfied	45	31%
Neutral	46	32%
Dissatisfied	9	6%
Highly Dissatisfied	2	1%
Total	145	100.0%

CHART 4.1.24: OFFICERS' INTERACT IN TERMS OF IDEAS AND FEELINGS

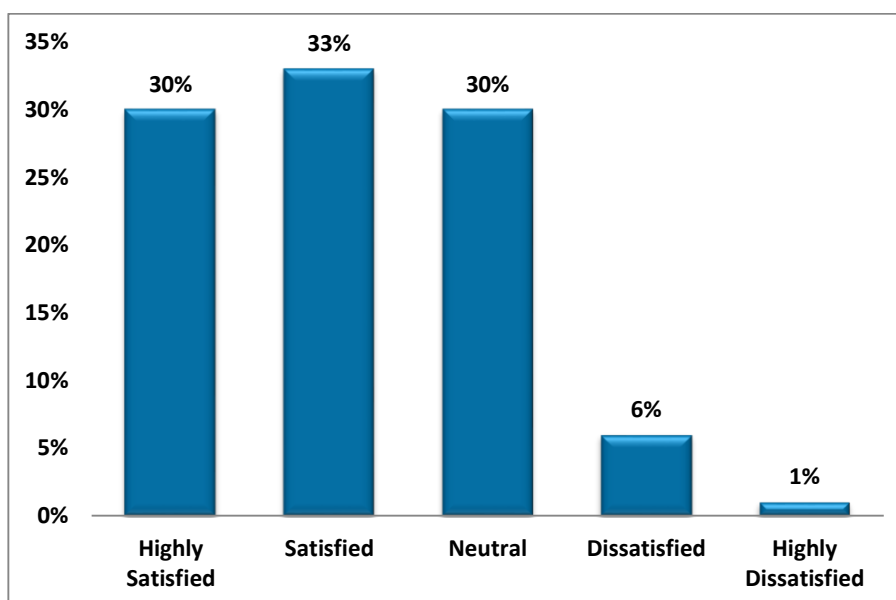


Interpretation: 30% respondents are highly dissatisfied with the officers of department interacting in terms of ideas and feelings, 31% of them are dissatisfied with this, 32% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.

TABLE 4.1.25: SATISFACTION WITH THE CLARITY IN COMMUNICATION OR GRIEVANCE BY SUPERIOR

Frequency	No.of Respondents	Percentage
Highly Satisfied	44	30%
Satisfied	47	33%
Neutral	44	30%
Dissatisfied	8	6%
Highly Dissatisfied	2	1%
Total	145	100.0%

CHART 4.1.25: SATISFACTION WITH THE CLARITY IN COMMUNICATION OR GRIEVANCE BY SUPERIOR

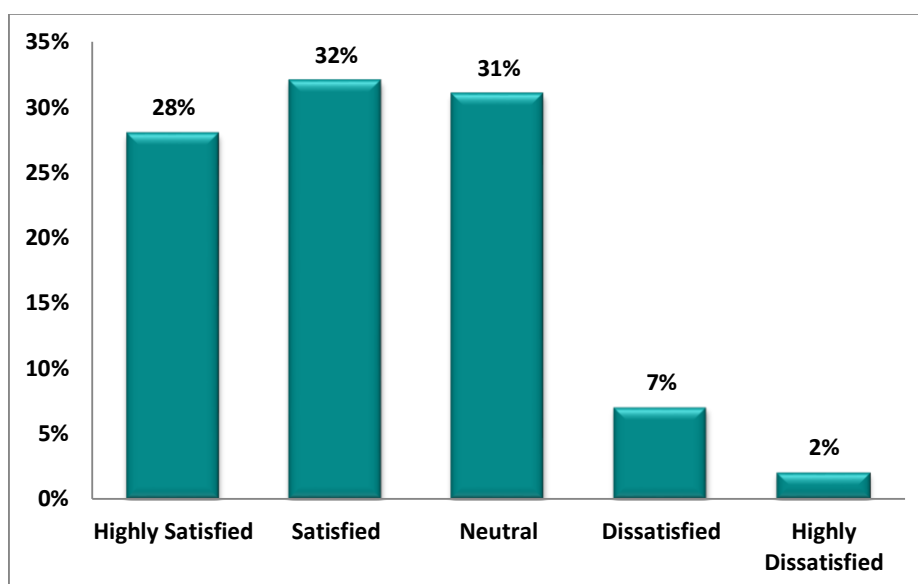


Interpretation: 30% respondents are highly dissatisfied with the clarity of communication or grievances handled by superior, 33% of them are dissatisfied with this, 30% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.

TABLE 4.1.26: SATISFACTION WITH GRIEVANCE HANDLING BY SUPERIOR

Frequency	No.of Respondents	Percentage
Highly Satisfied	40	28%
Satisfied	47	32%
Neutral	45	31%
Dissatisfied	10	7%
Highly Dissatisfied	3	2%
Total	145	100.0%

CHART 4.1.26: SATISFACTION WITH GRIEVANCE HANDLING BY SUPERIOR

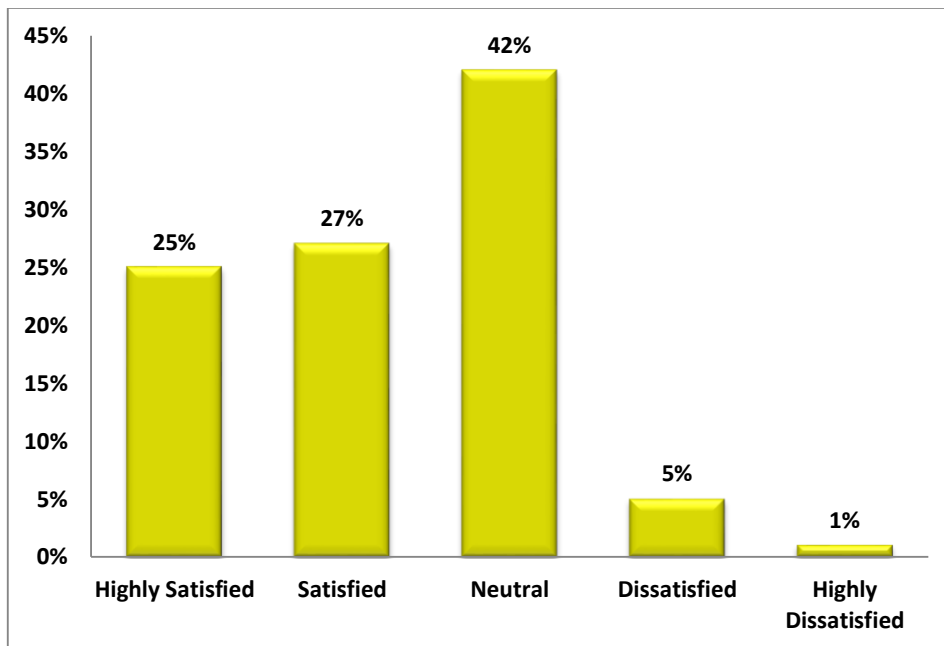


Interpretation: 28% respondents are highly dissatisfied with the grievances handling procedure by the superior, 32% of them are dissatisfied with this, 31% of the respondents are neutral towards this, 7% respondent are found to be satisfied and rest 2% of them are highly satisfied.

TABLE 4.1.27: LEVEL OF JOB INVOLVEMENT IS HIGH

Frequency	No. of Respondents	Percentage
Highly Satisfied	36	25%
Satisfied	39	27%
Neutral	61	42%
Dissatisfied	7	5%
Highly Dissatisfied	2	1%
Total	145	100.0%

CHART 4.1.27: LEVEL OF JOB INVOLVEMENT IS HIGH

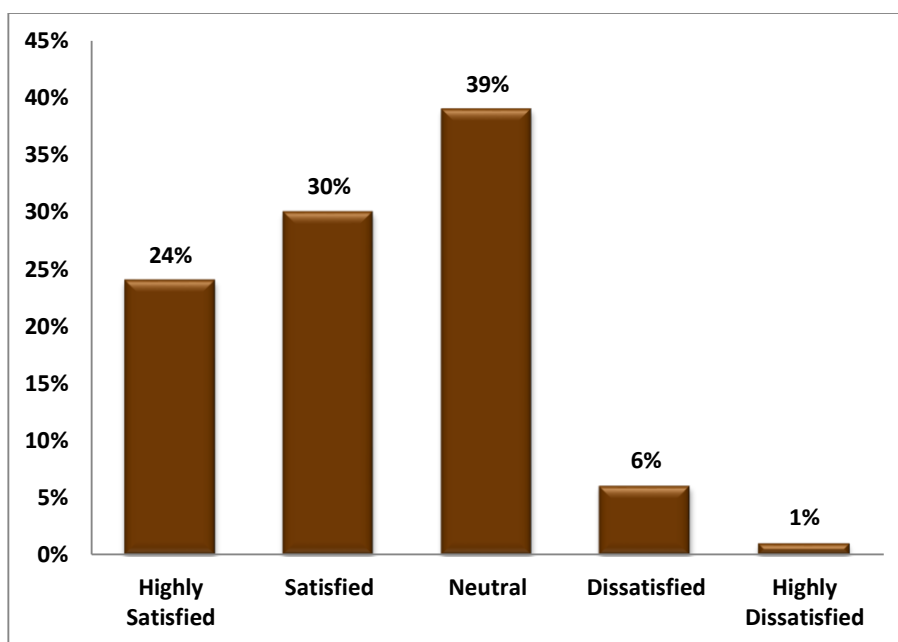


Interpretation: 25% respondents are highly dissatisfied with the high level of job involvement, 27% of them are dissatisfied with this, 42% of the respondents are neutral towards this, 5% respondent are found to be satisfied and rest 1% of them are highly satisfied.

TABLE 4.1.28: SATISFACTION WITH THE PERFORMANCE APPRAISAL

Frequency	No. of Respondents	Percentage
Highly Satisfied	35	24%
Satisfied	43	30%
Neutral	56	39%
Dissatisfied	9	6%
Highly Dissatisfied	2	1%
Total	145	100.0%

CHART 4.1.28: SATISFACTION WITH THE PERFORMANCE APPRAISAL

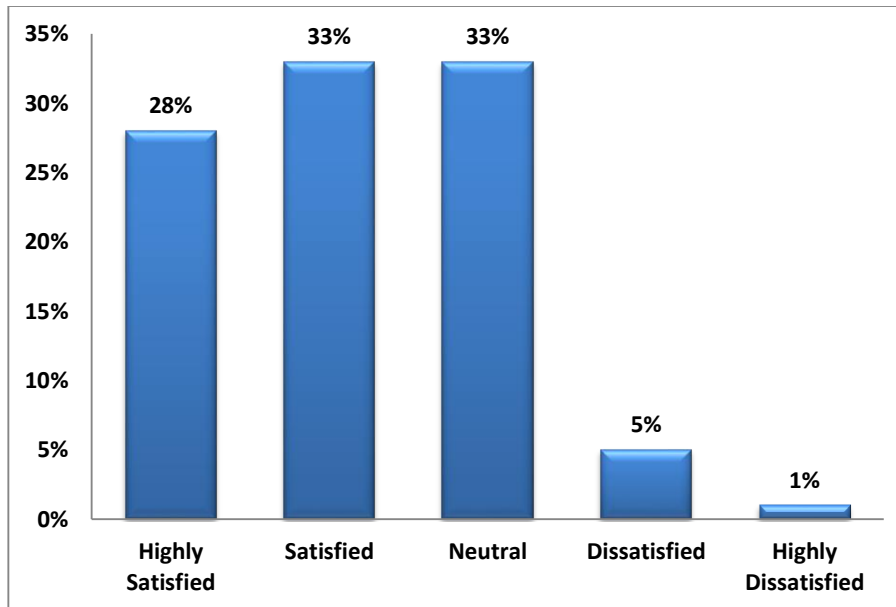


Interpretation: 24% respondents are highly dissatisfied with the performance appraisal in the department, 30% of them are dissatisfied with this, 39% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.

TABLE 4.1.29: SATIAFACTION WITH THE WORK LOAD

Frequency	No.of Respondents	Percentage
Highly Satisfied	41	28%
Satisfied	48	33%
Neutral	47	33%
Dissatisfied	7	5%
Highly Dissatisfied	2	1%
Total	145	100.0%

CHART 4.1.29: SATIAFACTION WITH THE WORK LOAD



Interpretation: 28% respondents are highly dissatisfied with the fixation of work load in the cyber-crime department, 33% of them are dissatisfied with this, 33% of the respondents are neutral towards this, 5% respondent are found to be satisfied and rest 1% of them are highly satisfied.

4.2 CORRELATION

HYPOTHESIS:

H0 (Null Hypothesis): There is no significant difference between Age and Comfortable with the Working Hours.

H1 (Alternate Hypothesis): There is a significant difference between Age and Comfortable with the Working Hours.

Table 4.2.1: Showing Age and Comfortable with the Working Hours

Descriptive Statistics			
	Mean	Std. Deviation	N
Age	2.52	1.355	145
Comfortable with the Working Hours	3.85	1.076	145

Correlations			
		Age	Comfortable with the Working Hours
Age	Pearson Correlation	1	-.460**
	Sig. (2-tailed)		.000
	N	145	145
Comfortable with the Working Hours	Pearson Correlation	-.460**	1
	Sig. (2-tailed)	.000	
	N	145	145

** . Correlation is significant at the 0.01 level (2-tailed).

Interpretation:

The p-value is 0.000 which is lesser than the alpha value (0.05), hence alternate hypothesis (H1) is accepted. Therefore, there is a significant difference between Age and Comfortable with the Working Hours.

HYPOTHESIS:

H0 (Null Hypothesis): There is no significant difference between Age and Job is affecting the Health.

H1 (Alternate Hypothesis): There is a significant difference between Age and Job is affecting the Health.

Table 4.2.2: Showing Age and Job is Affecting the Health

Descriptive Statistics			
	Mean	Std. Deviation	N
Age	2.52	1.355	145
Job is Affecting the Health	3.77	1.032	145

Correlations			
		Age	Job is Affecting the Health
Age	Pearson Correlation	1	-.342**
	Sig. (2-tailed)		.000
	N	145	145
Job is Affecting the Health	Pearson Correlation	-.342**	1
	Sig. (2-tailed)	.000	
	N	145	145

** . Correlation is significant at the 0.01 level (2-tailed).

Interpretation:

The p-value is 0.000 which is lesser than the alpha value (0.05), hence alternate hypothesis (H1) is accepted. Therefore, there is a significant difference between Age and Job is affecting the Health.

4.3 CHI SQUARE

Chi-Square between age of the respondents and their opinion to be a part of cyber-crime department

To find the reliability of the collected data Chi-square test has to be conducted, required hypothesis is the null hypothesis

Null Hypothesis:

H_0 = There is no dependency between age of the respondents and their opinion to be a part of cyber-crime department

Alternate Hypothesis:

H_1 = There is a dependency between age of the respondents and their opinion to be a part of cyber-crime department

Table 4.3.1: Chi-Square between age of the respondents and their opinion to be a part of cyber-crime department

Age * Proud Crosstabulation								
			Proud					Total
			Highly Dissatisfi ed	Dissatis fied	Neutra l	Satisfi ed	Highly Satisfie d	
A g e	Less than 25 Years	Count	5	3	8	0	0	16
		Expected Count	5.1	4.5	5.3	.8	.3	16.0
	25-30 Years	Count	15	10	15	2	2	44
		Expected Count	14.0	12.4	14.6	2.1	.9	44.0
	31-35 Years	Count	15	10	8	2	1	36
		Expected Count	11.4	10.2	11.9	1.7	.7	36.0
	36-40 Years	Count	10	6	8	3	0	27
		Expected Count	8.6	7.6	8.9	1.3	.6	27.0
	Above 40 Years	Count	1	12	9	0	0	22
		Expected Count	7.0	6.2	7.3	1.1	.5	22.0
Total		Count	46	41	48	7	3	145
		Expected Count	46.0	41.0	48.0	7.0	3.0	145.0

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	23.288 ^a	16	.106
Likelihood Ratio	27.286	16	.038
Linear-by-Linear Association	.106	1	.745
N of Valid Cases	145		
a. 11 cells (44.0%) have expected count less than 5. The minimum expected count is .33.			

Interpretation: Chi square value of $\chi^2 (16) 0.106 > \text{significance } (0.005)$ and the accepted is alternate Hypothesis. Hence there is a significant relationship between age of the respondents and their opinion to be a part of cyber-crime department

4.4 ANOVA

ONE WAY ANOVA TEST

Hypothesis

Between role immediately prior to joining the cyber- crime unit and their satisfaction towards their work load

Null Hypothesis:

H_0 = There is no statistically significant relationship between role immediately prior to joining the cyber- crime unit and their satisfaction towards their work load

Alternate Hypothesis:

H_1 = There is a statistically significant relationship between role immediately prior to joining the cyber- crime unit and their satisfaction towards their work load

Table 4.4.1: Between role immediately prior to joining the cyber- crime unit and their satisfaction towards their work load

Descriptives								
Workload								
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
General 'patrol' or 'response' officer	39	2.3333	.98230	.15729	2.0149	2.6518	1.00	5.00
Detective or investigative background	48	2.2083	.89819	.12964	1.9475	2.4691	1.00	4.00
Data analyst or intelligence	46	2.0217	.90650	.13366	1.7525	2.2909	1.00	4.00
First position in the Police	7	2.4286	1.39728	.52812	1.1363	3.7208	1.00	5.00
Other internal Police specialist unit	5	1.8000	.83666	.37417	.7611	2.8389	1.00	3.00
Total	145	2.1793	.94772	.07870	2.0237	2.3349	1.00	5.00

ANOVA					
Workload					
	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	3.262	4	.816	.906	.463
Within Groups	126.076	140	.901		
Total	129.338	144			

Interpretation: This is the table that shows the output of the ANOVA analysis and we have no statistically significant difference between our group means. We can see that the significance level is 0.463 ($p = .463$), which is more than 0.005, therefore, there is statistically significant relationship between role immediately prior to joining the cyber- crime unit and their satisfaction towards their work load

4.5 REGRESSION

HYPOTHESIS:

H0 (Null Hypothesis): There is no significant difference between Compensation Earned and Satisfaction with Reward System.

H1 (Alternate Hypothesis): There is a significant difference between Compensation Earned and Satisfaction with Reward System.

Table 4.5.1: Showing Compensation Earned and Satisfaction with Reward System

Model Summary									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.897 ^a	.804	.803	.435	.804	586.547	1	143	.000

a. Predictors: (Constant), Compensation Earned

ANOVA ^a						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	111.083	1	111.083	586.547	.000 ^b
	Residual	27.082	143	.189		
	Total	138.166	144			

a. Dependent Variable: Satisfaction with Reward System

b. Predictors: (Constant), Compensation Earned

Coefficients ^a						
Model		Unstandardized Coefficients		Standardized Coefficients	T	Sig.
		B	Std. Error	Beta		
1	(Constant)	.758	.136		5.585	.000
	Compensation Earned	.820	.034	.897	24.219	.000

a. Dependent Variable: Satisfaction with Reward System

Interpretation:

The p-value is 0.000 which is lesser than the alpha value (0.05), hence alternate hypothesis (H1) is accepted. Therefore, there is a significant difference between Compensation Earned and Satisfaction with Reward Sits.

CHAPTER 5

FINDINGS & CONCLUSION

5.1 FINDINGS OF THE STUDY

- 21% respondents are ITI / diploma holders, 66% of them are graduates, and 13% of the respondents are having other qualifications
- 11% respondents are having less than 25 years of experience, 30% of them 25-30 years old, 25% of them are 31-35 years old, and 19% of the respondents are 36-40 Years old and rest 15% of them are more than 40 years old
- 17% respondents have less than 1 year experience, 29% of them have 1-3 years of experience, 23% of them have 4-8 years of experience, 17% respondents have 9-12 years of experience and rest 13% have more than 12 years of experience
- 22% respondents are earning 10,000-20,000 per month, 23% respondents' income per month is 20,001-25,000, 32% of them are earning 25,001-30,000 per month, 23% respondents are earning more than 30,000 per month
- 27% respondents said their role immediately before joining the cyber-crime unit was General 'patrol' or 'response' officer, 33% of them said they were in the detective or investigative background with this, 32% of the respondents were in data analyst or intelligence unit, 5% respondents were working as a police and rest 3% of them were working on other internal Police specialist unit.
- 31% respondents volunteered or self-nominated themselves for their present role, 27% of them said their colleague recommended for that role, 35% of the respondents said they were recommended by their superior for this role, 6% respondent said they were seconded for that role and rest 1% of them said they were unsure about that
- 27% respondents are highly dissatisfied with the comfortable working hours, 33% of them are dissatisfied with this, 32% of the respondents are neutral towards this, 5% respondent are found to be satisfied and rest 3% of them are highly satisfied.
- 31% respondents are highly dissatisfied with the prospective and interesting job, 27% of them are dissatisfied with this, 35% of the respondents are neutral

towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.

- 32% respondents are highly dissatisfied with the part of the cybercrime department, 28% of them are dissatisfied with this, 33% of the respondents are neutral towards this, 5% respondent are found to be satisfied and rest 2% of them are highly satisfied.
- 25% respondents are highly dissatisfied with the working hours and working shift, 29% of them are dissatisfied with this, 39% of the respondents are neutral towards this, 4% respondent are found to be satisfied and rest 3% of them are highly satisfied.
- 32% respondents are highly dissatisfied with the job that is affecting their health, 27% of them are dissatisfied with this, 34% of the respondents are neutral towards this, 5% respondent are found to be satisfied and rest 2% of them are highly satisfied.
- 32% respondents are highly dissatisfied with the physical working conditions of the department like Light, A/C, air etc. 31% of them are dissatisfied with this, 31% of the respondents are neutral towards this, 5% respondent are found to be satisfied and rest 1% of them are highly satisfied
- 30% respondents are highly dissatisfied with the less crowded and clean workplace, 30% of them are dissatisfied with this, 33% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied
- 22% respondents are highly dissatisfied with the workplace giving less emphasis on the equipment than the individual, 31% of them are dissatisfied with this, 39% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 2% of them are highly satisfied.
- 27% respondents are highly dissatisfied with the adaptable and comfortable workplace, 30% of them are dissatisfied with this, 36% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.
- 27% respondents are highly dissatisfied with the fact that they do not neglect their health due to job, 30% of them are dissatisfied with this, 36% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.

- 22% respondents are highly dissatisfied with the energy and time that the officers spend on the job does not affect their life adversely, 30% of them are dissatisfied with this, 41% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.
- 30% respondents are highly dissatisfied with the necessary safety equipment provided by the cyber-crime department, 30% of them are dissatisfied with this, 32% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 2% of them are highly satisfied.
- 26% respondents are highly dissatisfied with the department's welfare policies, 34% of them are dissatisfied with this, 32% of the respondents are neutral towards this, 4% respondent are found to be satisfied and rest 4% of them are highly satisfied.
- 28% respondents are highly dissatisfied with the compensation provided by the cyber-crime department help them to maintain a socially desirable standard of living, 33% of them are dissatisfied with this, 32% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.
- 27% respondents are highly dissatisfied with the rewards system their cyber-crime department, 32% of them are dissatisfied with this, 36% of the respondents are neutral towards this, 4% respondent are found to be satisfied and rest 1% of them are highly satisfied.
- 28% respondents are highly dissatisfied with the co-operation within the co-workers, 33% of them are dissatisfied with this, 31% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 2% of them are highly satisfied.
- 25% respondents are highly dissatisfied with the working as a team in the department, 32% of them are dissatisfied with this, 38% of the respondents are neutral towards this, 4% respondent are found to be satisfied and rest 1% of them are highly satisfied.
- 30% respondents are highly dissatisfied with the officers of department interacting in terms of ideas and feelings, 31% of them are dissatisfied with this, 32% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.

- 30% respondents are highly dissatisfied with the clarity of communication or grievances handled by superior, 33% of them are dissatisfied with this, 30% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.
- 28% respondents are highly dissatisfied with the grievances handling procedure by the superior, 32% of them are dissatisfied with this, 31% of the respondents are neutral towards this, 7% respondent are found to be satisfied and rest 2% of them are highly satisfied.
- 25% respondents are highly dissatisfied with the high level of job involvement, 27% of them are dissatisfied with this, 42% of the respondents are neutral towards this, 5% respondent are found to be satisfied and rest 1% of them are highly satisfied.
- 24% respondents are highly dissatisfied with the performance appraisal in the department, 30% of them are dissatisfied with this, 39% of the respondents are neutral towards this, 6% respondent are found to be satisfied and rest 1% of them are highly satisfied.
- 28% respondents are highly dissatisfied with the fixation of work load in the cyber-crime department, 33% of them are dissatisfied with this, 33% of the respondents are neutral towards this, 5% respondent are found to be satisfied and rest 1% of them are highly satisfied.

5.2 SUGGESTIONS

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,

- ✎ Formulate the policy on WLB of police officers based on the company's vision & mission's statement.
- ✎ Form a committee that comprises of representatives from management as well as workers category.
- ✎ Conduct workshops to enhance knowledge and necessity of this policy.
- ✎ Communicate the policy to all the police officers.
- ✎ Implement the policy of maintain regular feedbacks & suggestions.
- ✎ Register and record each activity of the committees/Taskforce.
- ✎ Update any changes that have been made to all police officers.
- ✎ Make the policy reachable and understandable by all.
- ✎ No specific psychometric tool was previously available to measure the issues of police officers' Indian society, an assessment tool like Wheel of Life, Police officer Support Network (ESN) and other self-assessment tools are to be introduced in the company
- ✎ Human resource professionals and management consultants can also use these scales to redress WLB issues among police officers'
- ✎ By analyzing the major dimensions of the WLB issues of the police officers one can understand the areas in which the entrepreneur needs remediation and provide advice accordingly.
- ✎ **Only paper work no implementation:** The organization has the policies only on paper. There is very less concern for the implementation of the policies.
- ✎ **Lack of communication:** Communication about work/life programs is essential. Although an organization may offer a rich menu of work/life benefits, the desired effect—yielding positive business results—is unlikely to occur if police officers do not know about the programs or understand them.
- ✎ **Team Work:** Introducing, operating and implementing work-life balance requires collaborative working and is very much a holistic process.

- ✍ **Time Consuming:** Implementing a WLB strategy takes time. Timescales for implementation need to be realistic

5.3 CONCLUSION

The first historical events related to cybercrime, have its roots when the initial computer networks were set up and at the same time due to the growth of personal computing; these events marked an expansion of the cyber criminality. The pioneer hackers were conceived at the MIT (Massachusetts Institute of Technology) in 1960 and on November 20, 1963, they were mentioned by an MIT student (The Tech: MIT Student Journal -1963). As years passed by, the term acquired a different connotation; linked to cause damages to information systems and computers. As a concluding note, the current study found that work-related attitudes matter in predicting job satisfaction of cyber-crime offices. We also found that there were similarities, as well as important differences, in the positive and negative features of the job across levels of job satisfaction. It should be encouraging to know for high level offices, researchers, and observers that police officers as a group are generally satisfied with their job (i.e., only 5.3% were unsatisfied), and more importantly, the most frequently cited response regarding what is liked best about the police occupation (irrespective of satisfaction level) was the ability to help people. 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

- ✍ Ajayi (2016), Challenges to enforcement of cyber-crimes laws and policy, Journal of Internet and Information Systems, Vol. 6(1), pp. 1-12, August 2016
- ✍ Jason R. C. Nurse (2018), Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit, The Oxford Handbook of Cyber psychology (2018/19)
- ✍ K. Choi., & C. S. Lee (2018) International Journal of Cyber security Intelligence and Cybercrime, 1 (1), 1-4.
- ✍ Parti, E., Kiss, T., & Kopl'anyi, G. (2018). Architecture of aggression in cyberspace: Testing cyber social deviance in youth utilizing the Bryant-Smith Aggression Scales. International Journal of Cyber security Intelligence and Cybercrime, 1(1), 57-70
- ✍ Giever, D. (2018). "An argument for interdisciplinary programs in cyber-security, International Journal of Cyber-security Intelligence and Cybercrime, 1(1), 71-76
- ✍ John Ashcroft (2002), Satisfaction with Police—What Matters? U.S. Department of Justice Office of Justice Programs National Institute of Justice
- ✍ 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
- ✍ Al-Suwaidi et. al. – Estimating Causes of Cyber Crime: Evidence from Panel Data FGLS Estimator, International Journal of Cyber Criminology – ISSN: 0974 – 2891, July – December 2018. Vol. 12(2): 392–407
- ✍ McGuire, M. (2012) organized crime in the digital age London, UK: John Grieve Centre for Policing and Security
- ✍ Ciancaglini, V., Balduzzi, M., Goncharov, M., & McArdle, R. (2013). Deepweb and Cybercrime, Trend micro report
- ✍ Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies, Third World Quarterly, 31(7), 1057-1079
- ✍ Jaishankar, K. (2018). Cyber Criminology as an Academic Discipline: History, Contribution and Impact. International Journal of Cyber Criminology, 12(1), 1-8.

- ✍ B. Rajesh, Y.R. Janardhan Reddy, B. Dillip Kumar Reddy (2015), A Survey Paper on Malicious Computer Worms, International Journal of Advanced Research in Computer Science & Technology (IJARCST 2015)
- ✍ Kok Yeow Chong, Daisy Mui Hung Kee (2019), Job Satisfaction and performance of police officers in Penang, International Conference on Business Sustainability and Innovation, The European Proceedings of Social & Behavioural Sciences, EPSBS, ISSN: 2357-1330
- ✍ L. Lokesh, Swati Patra & S. Venkatesan (2016), Job Satisfaction among Police Personnel: A Socio-Demographic Study
- ✍ Nina Tomaževič, Janko Seljak, Aleksander Aristovnik (2015), Factors Influencing Police officer Satisfaction in the Police Service: The Case of Slovenia
- ✍ Regner Sabillon, Jeimy Cano, Victor Cavaller, Jordi Serra (2016), Cybercrime and Cybercriminals: A Comprehensive Study, International Journal of Computer Networks and Communications Security VOL. 4, No. 6, June 2016, 165–176
- ✍ Eugene A. Paoline III¹ and Jacinta M. Gau (2020), an Empirical Assessment of the Sources of Police Job Satisfaction, Police Quarterly 2020, Vol. 23(1) 55–81, the Author(s) 2019
- ✍ Johnson, R. R. (2012). Police officer job satisfaction: A multidimensional analysis. Police Quarterly, 15(2), 157–176
- ✍ Andhika Pratama and Fauzi Adi Rafrastara (2012), Computer Worm Classification, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 10, No.4, April 2012

APPENDIX I

QUESTIONNAIRE

1. Name : _____

2. Educational qualification:

a) Diploma b) Graduate c) Post Graduate

3. Age:

a) Less than 25 Years b) 25-30 Years c) 31-35 Years d) 36-40 Years e) Above 40 years

4. Work Experience in cyber-crime unit:

a) Less than 1 Year b) 1-3 Years c) 4-8 Years d) 9-12 Years e) More than 12 years

5. Income Level:

a) Less than 10,000 b) 10,000 - 20,000 c) 20,001-25,000 d) 25,001-30,000 e) More than 30,000

6. What is your role immediately prior to joining the cyber- crime unit?

a) General 'patrol' or 'response' officer b) Detective or investigative background
c) Data analyst or intelligence d) First position in the Police
e) Other internal Police specialist unit

7. In which circumstance through which you joined the cyber-crime unit?

a) I volunteered or self-nominated for the role b) A colleague recommended the role
c) A superior recommended me for the role d) I was seconded to the role e) Unsure

Criteria Description	Highly Satisfied	Satisfied	Neutral	Dissatisfied	Highly dissatisfied
----------------------	------------------	-----------	---------	--------------	---------------------

Q.No	Working conditions	HS	S	N	DS	HDS
8	Working hours are comfortable					
9	Job is interesting and prospective					
10	Proud to be part of cyber-crime department					
11	Satisfied with the working hours					
12	Job is not affecting officials' health					
	Physical Environment					
13	Physical working conditions(Light,A/C,Airetc)					
14	Workplace is less crowded and clean.					

15	The work environment gives less emphasis on the equipment than the individual.					
16	The environment is more adaptable and comfortable					
	Health, welfare and safety standards					
17	I do not neglect my health due to my job					
18	The energy and time that spent on job does not affect life adversely					
19	Safety equipment are necessary are provided by the cybercrime department					
20	I am fully satisfied with company welfare.					
	Compensation and rewards					
21	Compensation helps to maintain a socially desirable standard of living					
22	Satisfied with the rewards system in of the cybercrime department					
	Superior Subordinate Relationship					
23	Cooperate with co-officers.					
24	Working as a team is not problem here					
25	Officials interact in terms of ideas and feelings.					
26	Communication or grievances by superior is clear and satisfactory.					
27	Grievances handling procedure by the superior is satisfactory.					
	Job Involvement					
28	Officers' level of job involvement is high					
29	Performance appraisal in the organization is satisfactory					
30	Work load fixed is satisfactory					

31. As a part of the cyber-crime department, your suggestions to enhance the Job satisfaction among officers

--

APPENDIX ARTICLE II

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

Dr. BHUVANESWARI G

bhuvanewarisomsgmail.com

DEAN

SCHOOL OF MANAGEMENT STUDIES

*SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY, CHENNAI –
600119*

Mr. ARAVINDAN E

aravind02041998@gmail.com

STUDENT

SCHOOL OF MANAGEMENT STUDIES,

*SATHYABAMA INSTITUTE OF SCIENCE AND TECHNOLOGY, CHENNAI -
600119*

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.

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.

STATEMENT OF THE PROBLEM

Cyber-crime is the new challenge for the Indian society, industry and the law enforcement and the entire criminal justice system as a whole. The anonymous nature of the Internet makes it an attractive medium to commit crimes and frauds. Cyber-crime is not confined to any national boundary. The police personnel, the prosecutors and the lower judiciary need to be educated to fight cyber-crimes. This can be effectively achieved by organizing periodic conferences, seminars and workshops, training programmes. Sometimes we often wonder how wired connected we are with each other. Almost everything in our life is connected to some kind of technology and its gadgets. But imagine what a hacker can do to our life. The Commission on Crime Prevention and Criminal Justice (CCPCJ) of the United Nations, with its headquarters in Vienna, has been exercised over how to

prevent and control high technology and computer-related crime. The commission is convinced that one way of doing this is to forge closer links between nations so that the cyber-criminal is relentlessly pursued across frontiers.

NEED FOR THE STUDY

This research aims to determine how police officer satisfaction, retention, loyalty influence the cyber-crime department and performance of police officers working in Cyber –criminality department in Tamil Nadu Police Department. This report intends to prove, that satisfied officers tend to be loyal and committed to the department and it has a positive influence towards the performance of Cybercrime branch. The results would reveal that the increase of job satisfaction makes their intention to continue their work with complete satisfaction.

OBJECTIVES OF THE STUDY

- To identify the challenges faced by officers investigating cyber-crime.
- To know their level of satisfaction towards their job
- To define types of cyber-crimes against individuals
- To analyse the factors involved in cyber-crime reporting and investigation
-

REVIEW OF LITERATURE

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.

RESEARCH METHODOLOGY

Research Design: The research design adopted for this study is Exploratory Research.

Sources of Data:

For the purpose of the study, both primary and secondary data has been obtained from officers of police department and with the help of the published information provided by the police officers working for cyber-crime department

Primary data is collected by issuing a well-designed questionnaire to the officers and their opinions and suggestions were sought with the help of the questionnaire.

Secondary data is gathered with the help of the literature that has been obtained from the department in the various forms as such magazines, journals, annual report and additional information. Apart from the questionnaire I took the help of secondary data sources as:

- Records and documents
- Magazines and other brochures published
- Newspapers and other data sources
- Websites.

Sampling Design: 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

Sample Size: 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: Area of survey is Chennai

Tools & Techniques:

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.

- Correlation
- Chi-square analysis

- Anova

RESULT ANALYSIS AND DISCUSSION

CORRELATION

H0 (Null Hypothesis): There is no significant difference between Age and Comfortable with the Working Hours.

H1 (Alternate Hypothesis): There is a significant difference between Age and Comfortable with the Working Hours.

Showing Age and Comfortable with the Working Hours

Descriptive Statistics

	Mean	Std. Deviation	N
Age	2.52	1.355	145
COMFORTABLE WITH THE WORKING HOURS	3.85	1.076	145

Correlations

		Age	COMFORTABLE WITH THE WORKING HOURS
Age	Pearson Correlation	1	-.460**
	Sig. (2-tailed)		<.001
	N	145	145
COMFORTABLE WITH THE WORKING HOURS	Pearson Correlation	-.460**	1
	Sig. (2-tailed)	<.001	
	N	145	145

**. Correlation is significant at the 0.01 level (2-tailed).

Inference:

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 Comfortable with the Working Hours.

CHI-SQUARE

HYPOTHESIS:

H0 (Null Hypothesis): There is no significant difference between Role immediately prior to joining the Cyber-Crime unit and Job is interesting & prospective.

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

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.

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	1.638	<.001
	Cramer's V	.819	<.001
N of Valid Cases		145	

Inference:

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.

ANOVA

HYPOTHESIS:

H0 (Null Hypothesis): There is no significant difference between Age and Working as a Team is not a Problem.

H1 (Alternate Hypothesis): There is a significant difference between Age and Working as a Team is not a Problem.

Table 4.4.1 Showing Age and Working as a Team is not a Problem

Descriptives								
WORKING AS A TEAM IS NOT A PROBLEM								
	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
					Lower Bound	Upper Bound		
25-30 Years	44	4.09	1.007	.152	3.78	4.40	3	5
31-35 Years	36	4.61	.494	.082	4.44	4.78	4	5
36-40 Years	27	4.00	.000	.000	4.00	4.00	4	4
Above 40 Years	22	3.00	1.380	.294	2.39	3.61	1	4
Less than 25 Years	16	3.00	.000	.000	3.00	3.00	3	3
Total	145	3.92	.997	.083	3.75	4.08	1	5

Tests of Homogeneity of Variances					
		Levene Statistic	df1	df2	Sig.
WORKING AS A TEAM IS NOT A PROBLEM	Based on Mean	222.557	4	140	<.001
	Based on Median	9.101	4	140	<.001
	Based on Median and with adjusted df	9.101	4	69.346	<.001
	Based on trimmed mean	181.044	4	140	<.001

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			

Inference:

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.

LIMITATIONS OF THE STUDY

- The study is restricted to Cyber-crime officers alone.
- Due to time constraint the sample size is restricted.
- The study considered only 145 samples.
- The officers could not contribute more time. Some of them are not willing to answer
- The research may not reveal exact results due to the bias answers of the officers

SUGGESTIONS

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,

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

- Ciancaglini, V., Balduzzi, M., Goncharov, M., & McArdle, R. (2013). Deepweb and Cybercrime, Trend micro report.
- Jaishankar, K. (2018). Cyber Criminology as an Academic Discipline: History, Contribution and Impact. International Journal of Cyber Criminology, 12(1), 1-8.
- sssK. Choi., & C. S. Lee. (2018). International Journal of Cybersecurity Intelligence and Cybercrime, 1 (1), 1-4.
- 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
- Kshetri, N. (2010). Diffusion and effects of cyber-crime in developing economies, Third World Quarterly, 31(7), 1057-1079.

