Empirical relationship between Victim's occupation and their knowledge of Digital Forensic

Nilakshi Jain
Pacific Academy of Higher Education and Research,
Shah and Anchor Kutchhi Engineering College,India
nilakshijain1986@gmail.com

Dr. Dhananjay R Kalbande
Computer Engineering Department
Sardar Patel Institute of Technology
Mumbai,India
k_dhananjay@yahoo.com

Priyanka Sharma
Shah and Anchor Kutchhi Engineering College
Mumbai, India
sharma.priyanka25007@gmail.com

ABSTRACT
Computer crime also popularly known as Cybercrime has escalated to such a huge extent that it is now posing a threat to various industries, educational universities and professional organizations as well. The law enforcement agencies, police departments and crime branch units have acknowledged the upsurge in digital crime cases and they have begun to deploy measures to curb this evil phenomenon. In this paper, we inspect about the awareness of digital crime among the general public and illustrate an overview of Cybercrime, with the motive of highlighting the necessity to restrain the impact of cybercrime all over the world. This paper examines the rise in number of cybercrimes in India and takes into consideration the analytical traits of the offenders who commit such crimes. The paper banks on the information obtained from different sects of our country. The experimentation results depict that the top four cyber crimes committed in the past few years such as Internet frauds, data theft, cyber piracy and crime sex were all spread across the internet. The output reveals that cyber crime not only encompasses the internet but it has already expanded across all communities worldwide. The soaring crime rate is a major concern as it is indicative of the huge amount of cyber crime cases enrolled in recent years. The objective of this paper is to provide some guidelines to cybercrime analysts, government organizations, and educational universities.

General Terms
Cyber Crime, Digital Forensic

Keywords
Cyber Crime, Law, Internet Crime, Awareness

1. INTRODUCTION

Computers are definitely the most popular electronic gadgets as they are being extensively used in various fields like conserving private data and maintaining databases with the help of personal computers, carrying out space missions and ensuring the smooth functioning of industries and organizations with the help of supercomputers.

Due to the recent advancements in the field of technology, the communication network has expanded because of which a number of people have gained access to the information available on these computers. In case of large business and government organizations the uncontrolled access to crucial information increases the vulnerabilities of the system. The inventors of internet would have hardly suspected that it could be used as a weapon for committing crimes. For cyber criminals it is practicable to discover the flaws in computers and take undue advantage of these weaknesses to gain access to top secret information about the respective industries and financial firms. Since computers have now become an inseparable part of our day to day life, it is essential to protect the information stored on them from unauthorized access, theft, deletion and adulteration.

Cybercrimes are turning out to be disastrous for mankind, communities, and public safety [1]. Many papers have demonstrated that cybercrimes also adversely affect e-commerce [2]. An attempt to create public awareness on cybercrimes is by motivating legal authorities to amend related laws [3], to begin funding academic education [4], and to provide financial aid for developing cybercrime detection tools [5, 6]. The term 'cyber crime' has not been defined in any Statute or Act by the Information Communication Technology (ICT). Cyber Crime apparently means criminal offences and incidences in any form. A generic definition of cyber crime could be "unlawful acts wherein the computer is utilized either as a tool or it is targeted or both".

CBI Manual defines cybercrime as [7]:

(i) Crimes that use computers to execute attacks and also involve conventional crimes.
(ii) Crimes that are targeted to attack computers.

There is a hike in the flow of information within various organisations because ICT has cropped up in the fields of social networking, cloud computing, mobile technology etc. This is diminishing the security and privacy of organizational data. An upsurge in computer and network-related misuse is caused by the looming activity in ICT-based environments[8]. A common employee can deploy easily available password cracking tools to gain unauthorised access to managerial account information, to steal valuable company resources and carry fraudulent transactions has become simple as a wide range of open source tools are freely available to achieve one's selfish motives [8].

DOI: http://dx.doi.org/10.1145/2909067.2909097*WIR '16*, March 21-22, 2016, Indore, India.
DOI: 10.1145/2909067.2909077

Cyber crime has come into picture as computers are no longer limited only to IT sector but also form an integral part of other communities[9]. There is an urgency for digital forensic investigation to detect the crime and secure the distressed communities.

The Digital Forensics comprises of four distinct communities, they are[10]:

- Military
- Business & Industry
- Law Enforcement
- Academia

Our Research reveals that cyber crime is not related to only IT sectors. The awareness should be spread in all fields and also there should be a single unified approach for digital forensic investigation and techniques deployed for investigation. This should be used in all four communities mentioned above. Based on the review of literature the hypothesis H1 can be defined as :

H1: There is no association between victim's occupation and the knowledge of digital forensic.

The digital forensic awareness should be transmitted across all fields not only in IT sectors. The next section describes the research protocol which we used during our research

2. RESEARCH PROTOCOLS

The instrument of survey has been used to carry out quantitative research [9] of gathering data, to examine and put forth the collected data we have used descriptive statistics. Since the result of the conducted survey must be an illustrative sample of the entire population a quantitative research technique was selected. For the purpose of data collection an online questionnaire survey (Google Online form) was generated and then the link for the same was forwarded via mail to all respondents who are likely to be associated with different organizations.

Link for online survey is :
https://docs.google.com/forms/d/133UTilEEEcyei0SgcXqYlHSbezewPgo-uVa9rrC-Eac/viewform?c=0&w=1

2.1 Research Questions

The research questions were derived from the literature [10-13] because the nature of the report was experimental. In order to discover the existent awareness about digital forensics and cyber crimes among various respondents the questionnaire provided a strong foundation. In our questionnaire we enquired about the simple meaning of digital forensics from an individual's perspective, the different types of cyber crimes emerging these days and the preventive measures that must be taken to keep a check on them. In the process of data collection the respondent name or designation is kept confidential.

2.2 Selection of Respondent/ Participants

The elementary target respondents for the survey were working professionals who are aware about computer related crimes and safety issues present within his/her organization. Typically, these were IT administrators, chief managers, IT security consultants and also people who are associated with Law agencies, Military, Industrial firms and Academic institutions. The fundamental sampling method adopted when choosing the sample for this survey was simple random sampling and total number of participants is (N=1000).

2.3 Data Analysis

For conducting the research, we used Microsoft Excel software program & Google form summary and derived the hypothesis that there is no relation between Victim's Occupation and the knowledge of digital forensic. To test the hypothesis we have asked some questions related to cyber crime to all participants. All questions are analyzed and represented in the form of Table.

a) The gender frequency distribution of the participant pool was as follows for Total no of participants (N)=1000:

Table 1. The Number of Individual Gender who participated in Survey

Gender	No of Participants
Male	570
Female	430
Transgender	0

In the survey total male are 570 and females are 430 who responded.

b) The education frequency distribution of the participant pool was as follows:

Table 2. Education Status of Respondents

Education	No of Participants
High School Diploma	120
Associate's Degree	150
Bachelor's Degree	200
Master's Degree	180
Doctoral Degree	100
Post Doctoral	150
Other	100

The above Table 2 explains the education lhiest dergree completed by participants eg from 1000 participants total 150 were post doctorate.

c) Frequency distribution for most affected computer user group from cyber crime of the participant pool was as follows:

Table 3. Number of Most affected Computer User Group

Computer User Group	No of Participants
Government agencies	240
Financial institutions	210
Educational institutions	100
Private sector	220
Law enforcement agencies	110
Personal users	120

According to respondent which group communities are highly effected by cyber crime Table 4 explains the exact count.

d) Cyber crime spreading status freequency distribution :

Table 4. Cyber Crime Growth in India

Cyber Crime Rate in India	No of Participants
Very Fast	620
Average	310
Very Slow	70

e) According to all above factors digital forensic knowledge for each participant's can be defined either as good or average :

Table 5. Digital Forensic Awareness level in each Group

Occupation	Average	Good
Academia	40	80
Business & Industry	130	250
Military	90	180
Law Enforcement	70	160

In Academia it has been observed that out of 120 respondent 40 Academician have Average knowledge about Digital Forensic and 80 have good knowledge about Digital Forensic. In Business & Industries it can be observed that out of 380 respondent 130 have average knowledge and 250 have good knowledge level. In Military where cyber crime is main threat out of 270 participants 90 have average knowledge about crime and securing mechanism and 180 haven good knowledge about the same. In law enforcement out of 230 respondent 70 have average knowledge and 160 have good knowledge about forensic and investigation .It can be seen still there is need for awareness of digital forensic in all communities .

3. HYPOTHESIS TESTING

The data was first evaluated and then analyzed using exploratory and descriptive Statistics. The result indicated that the data was approximately normal and Chi Square Test could be applied. To test hypothesis H1, Chi Square [14] was implemented to scan the relationship between the knowledge of digital forensic and the occupation of each respondent. Table 6 defined the observed frequency for the hypothesis.

Table 6: Observed Frequencies

Digital forensic Knowledge Based on Occupation			
Occupation	**Average**	**Good**	**Total**
Academia	40	80	**120**
Business & Industry	130	250	**380**
Military	90	180	**270**
Law Enforcement	70	160	**230**
Total	**330**	**670**	**1000**

Expected frequency (E) for each value of observed frequency (O) can be calculated using formula [15]:

E= (Row Total * Colum Total)/ N

Table 7: Expected Frequencies for Hypothesis 1

Digital forensic Knowledge Based on Occupation			
Occupation	**Average**	**Good**	**Total**
Academia	39.6	80.4	**120**
Business & Industry	125.4	254.6	**380**
Military	89.1	180.9	**270**
Law Enforcement	75.9	154.1	**230**
Total	**330**	**670**	**1000**

Using the expected frequency E and Observed Frequency O the Chi Square ($\chi 2$) can be calculated as :

$$\chi 2 = \sum (O-E)^2 / E$$

Table 8: Chi Square Calculation for Hypothesis 1

Observed Frequency (O)	Expected Frequency (E)	(O-E)2 / E	$\chi 2$
40	39.6	0.90042	6.94057
80	80.4	0.80019	
130	125.4	0.96871	
250	254.6	0.88311	
90	89.1	0.80099	
180	180.9	0.90447	
70	75.9	0.85682	
160	154.1	0.82589	

According to Table 7 the Chi square ($\chi 2$) = 6.94057 is output for

hypothesis H1.To test the hypothesis we require degree of freedom.

Degree of Freedom df = (No of Row – 1) (No of Colum -1)

Degree of freedom for our hypothesis can be calculated as

Degree of Freedom df = (4 – 1) (2 -1) =3

Check in Chi-Square distribution Table at df = 3. We use the 0.05 probability level as our **critical value** as per statistical convention. If the calculated chi-square value is less than the 0 .05 value, we accept the hypothesis.

Table 9: Chi Square Distribution Table

df	0.995	0.99	0.975	0.95	0.9	0.1	0.05	0.025	0.01
1	0	0	0.001	0.004	0.016	2.706	3.841	5.024	6.635
2	0.01	0.02	0.051	0.103	0.211	4.605	5.991	7.378	9.21
3	0.072	0.115	0.216	0.352	0.584	6.251	7.815	9.348	11.345
4	0.207	0.297	0.484	0.711	1.064	7.779	9.488	11.143	13.277
5	0.412	0.554	0.831	1.145	1.61	9.236	11.07	12.833	15.086
6	0.676	0.872	1.237	1.635	2.204	10.645	12.592	14.449	16.812
7	0.989	1.239	1.69	2.167	2.833	12.017	14.067	16.013	18.475
8	1.344	1.646	2.18	2.733	3.49	13.362	15.507	17.535	20.09
9	1.735	2.088	2.7	3.325	4.168	14.684	16.919	19.023	21.666
10	2.156	2.558	3.247	3.94	4.865	15.987	18.307	20.483	23.209
..	..	..	..	..	..	..	..	..	..

The calculated value of $\chi 2$ is 6.94057 and Chi square distributed table value at df 3 at probability level 0.05 is 7.815. Since our calculated $\chi 2$ is less than the table value we can conclude that the hypothesis holds true.

4. CONCLUSION

Results affirm the significance of awareness of digital forensic as an instrument to decrease/ prevent cyber crime. Therefore it can be stated that there is no relation between the Victim's Occupation and his knowledge of digital forensic. The underestimation of the impact that cyber crime can have on the society is due to the misconception about an individual's knowledge about digital forensic. The awareness and knowledge about issues of cyber crimes and digital forensic among the people is certainly related to their reaction when faced with crime incidences. Some people turn a blind eye to cyber crimes as they occur in virtual world and people consider such instances delusive. This happens because these people are not directly connected to the cyber world and have no information on the adverse effects of probable cyber crime attacks.

5. GUIDELINES

In this section, we will give some guidelines to organizations, society, and universities.

5.1 Organization

Administrations need to modify existing digital crime related laws and deploy skillful researchers to combat cyber crimes efficiently. As the current laws their enforcement and prosecution are less stringent, criminals are becoming fearless. To aid the police officers in battling cyber crimes there is a need to devise rigid laws. Digital forensic labs require more number of investigators having both practical and legal knowledge so that potent digital evidences are gathered accurately such that these evidences can be effectually used to prosecute the suspected criminal in the court of law[12][14].

5.2 Society

McCusker[10] brought to notice that only 1% of computer crimes are caused by intrusion. We can observe that there is a high percentage of unreported cybercrimes. The reason is either inadequacy of data security knowledge or the victims' desire to protect their prestige. Geer[8] emphasize that the knowledge of securing data is essential to people. With proper data security knowledge, people will be better at detecting cybercrime instances. After finding out cybercrimes, people and organizations must report them immediately to the concerned authorities. If a successful cybercrime attack is ignored or remains unreported then it may encourage the attacker to launch many more cyber crime attacks in near future. So, this paper advices that law enforcement agencies must shield the attacked organizations or individuals.

5.3 Education Department

It is frequently observed that after a criminal who committed cybercrime is arrested and made to stand in the court of law, they pretend to be unaware about the fact that their act was unauthorized and is considered to be a crime. People must not only learn to operate computer systems but at the same time they need to be educated about the fundamental laws related to proper use of computers. They must also be aware about the ethical use of technology. There is a vital need for boosting data ethics and ethical education programs in academia, and more scholars need to be involved in such events. It is never too late to educate and incorporate ethical values in researchers and other internet users, regardless of their age and the communities they belong to.

6. ACKNOWLEDGMENTS

It gives us immense pleasure to thank Dr. Dhananjay R Kalbande, our Guide for extending his support to carry out this hypothesis. We would like to articulate our deep sense of gratitude and thank him for guidance, help and useful suggestions, which helped us.

7. REFERENCES

[1] Sukha N, “Hacking and cybercrime”, Proceedings of the 1st Annual Conference on Information Security Curriculum Development-ACM, pp. 128-132, 2014.

[2] Serban, C. (2014). Partnership in social marketing programs. Socially responsible companies and non-profit organizations engagement in solving society’s problems. Amfiteatru Economic, XIII (29),pp. 104-116.

[3] Svensson, P. (2013). Nasdaq hackers target service for corporate boards. Retrieved from http://news.yahoo.com/s/ap/20110205/ap_on_hi_te/us_nasdaq_hackers

[4] Matthews, B. (2011). Computer Crimes: Cybercrime Information, Facts and Resources. Retrieved from http://www.thefreeresource.com/computer-crimes-cybercrimeinformation-facts-and-resources

[5] Balkin, J. M. et al. (2012). Cybercrime: digital cops in a networked environment. New York: New York University Press (NYU).

[6] Thomas, D., and Loader, B. (2013). Cybercrime: law enforcement, security and surveillance in the information age. London: Routledge

[7] Cordy E, “The legal regulation of e-commerce transactions”, Journal of American Academy of Business, vol. 2, no. 2, pp. 400-407, 2010.

[8] Geer D, “Security technologies go phishing”, Computer, vol. 38, no. 6, pp. 18-21, 2014.

[9]] McCrohan K, “Facing the threats to e-commerce”, The Journal of Business & Industrial Marketing, vol. 18, no. 2/3, pp. 133-145, 2014.

[10] McCusker R, “E-Commerce, Business and Crime: Inextricably Linked, Diametrically Opposed”, The Company Lawyer, vol. 23, no. 1, pp. 3-8, 2002.

[11] Cronan T, Foltz C, and Jones T. “Piracy, computer crime, and is misuse at the university”, Communications of the ACM, 49(6):85-90, 2006.

[12] Philippsohn S, “Trends in Cybercrime - an overview of current financial crimes on the Internet”, Computers & Security, vol. 20, no. 1, pp. 53-69, 2001

[13] Thomas D, and Loader B, “Introduction - Cybercrime: Law Enforcement, Security and Surveillance in the Information Age”, In Cybercrime: Law Enforcement, Security and Surveillance in the Information Age. Taylor & Francis Group, New York, 2000.

[14] Smith, A and Rupp W, “Issues in cyber security: understanding the potential risks associated with hackers”, Information Management and Computer Security, vol. 10, no. 4, pp. 178-83, 2002.

[15] Nilakshi Jain and Dr.Dhananjay R Kalbande ,Digital Forensic Framework using Feedback and Case History Keeper ,International Conference on Communication ,Information & Computing Technology ,pp 1-6 ,2015.

[16] Nilakshi Jain and Dr.Dhananjay R Kalbande ,Computer Forensic Tool using History and Feedback Approach , International Conference on Reliability, Infocom Technologies and Optimization ,pp 1-5 ,2015.