IMPACT: International Journal of Research in Humanities, Arts and Literature (IMPACT: IJRHAL)
ISSN (P): 2347-4564; ISSN (E): 2321-8878
Vol. 7, Issue 3, Mar 2019, 315-338

SAFEGUARDING ORGANIZATIONS IN INDIA AGAINST CYBERCRIME – THE CORPORATE FRAUDS & CRIMES SURVEY

Geetu Singal[1], Aparna Prashant Goyal[2] & B. Nagi[3]

[1]Research Scholar, MRIIRS, Manav Rachna University, Faridabad

[2]Professor & Dean, Faculty of Commerce & Business Management, MRIIRS Manav Rachna University, Faridabad

[3]Visiting Professor, Manav Rachna University, Faridabad

Received: 18 Feb 2019 **Accepted: 07 Mar 2019** **Published: 16 Mar 2019**

ABSTRACT

Cybercrime consists of activities undertaken by an individual or company that are done in a dishonest or illegal manner, and are designed to give an advantage to the perpetrating individual or company. Cyber-attacks are becoming more frequent in India. In 2017, approximately 53,000 cases of cybercrimes were reported and there were rise of about 10 per cent during 2018 as reported by two officials in the security establishment. It may be pointed out that almost 40 per cent of the attacks from January – May 2018 originated from China, and 25 percent from US; 13 per cent came from Pakistan and 9 per cent from Russia. For the present research paper, the data pertaining to fourteen factors which could help in preventing cybercrimes data were collected from 237 respondents. Out of the total respondents, 81 are the judges and 156 are the advocates. The average opinion of the respondents on the following three factors is little more than option 3 (Agree): Fake Websites, Hacking and Loose Security Measures. Taking proper or stringent security measures to protect the data and information would prevent cybercrimes. One has to be careful of fake websites and hacking activities in order to save the data and information from cybercrimes. The mean values of the perception of the respondents on following factors are nearing option 3 (Agree): Professional Networking, Social Media Sites, Unsecured Information, Privacy and Password Settings, Two Factor Authentication, Unsecured Public Wi-Fi, Recognized and Secured Payment Gateway, and Remote Access to Computer. These measures would help to maintain distance from the cybercrimes.

KEYWORDS: *Cyber-Crimes, Frauds, Perception, financial Institutions, Digital Transactions, Mobile Banking, E-Commerce*

INTRODUCTION

Cybercrime consists of activities undertaken by an individual or company that are done in a dishonest or illegal manner, and are designed to give an advantage to the perpetrating individual or company. Cyber crime or fraud schemes go beyond the scope of an employee's stated position, and are marked by their complexity and economic impact on the business, other employees and outside parties. A Russian-led posse in Spain ganged up to pump in viruses through internet into the computers of unsuspecting users in almost 30 countries in 2011-12. The viruses locked the computers. The fraudsters then sent online extortion messages, called ransom-ware, to the users in the form of fake police warnings, demanding $ 120 for unlocking their computers. However, the computers of even those who paid remained locked. This is cybercrime. A network was busted by the European Police Agency in early 2013. Around the world, homes and offices

were being broken into every day, not by breaking locks or forcing open windows, but by breaking into computers with a criminal intent by hacking and using malicious codes and other modes of cybercrime. Cybercrime is an economic offence carried out on computers via the internet. It involves the use of a large and ever-changing variety of tricks, and includes illegal downloading of files, data theft and loss, distribution of viruses, pharming (redirection of web information to another fraudulent site with a malevolent motive), phishing (theft of personal information such as bank passbook and accounts details) and computer hacking. Cybercrime is now a major risk, demanding immediate attention for any organization where internet is part of their business strategy, thus engulfing every enterprise. This paper focuses on the cyber crimes that have increased rampantly. A report appeared in the Hindustan Times on November 3, 2018 on 'Cyber attacks becoming more frequent in India'. It says that India may see 10 per cent rise in cyber attacks in 2018 as compared to approximately 53,000 such cases reported last year, according to two officials in the security establishment. There were about 50,000 attacks in 2016 and 49,000 in 2015, according to the country's Computer Emergency Response Team(CERT), considered the last line of defense for India's networks and infrastructure. The report further points out that almost 40 per cent of the attacks from January – May 2018 originated from China, and 25 percent from US according to CERT; 13 per cent came from Pakistan and 9 per cent from Russia. compared to last year, attacks from Pakistan and North Korea have increased this year , a senior official at CERT said on condition of anonymity. With critical infrastructure, including the country's financial markets and transport networks almost entirely are dependent on IT net works, cyber attacks can result in massive and widespread disruption. Cyber attack swill increase as the use of internet increases. But, the reporting of cyber attack is still very low in India, only 5 per cent of cyber attacks are reported to the authorities, said Jiten Jain, who collaborates with the government on cyber security and is also the CEO of Indian Info sec Consortium. According to data shared by Cyber Security Establishment with the Prime Minister's Office and which has been viewed by HT, most attacks were aimed at the country's financial networks and government arms, followed by power plants and grids. The report in HT also mentioned the threat of cybercrimes in the graphical presentation given in the box below: India witnessed about 53,000 cyber attacks in 2017. Officials say such cases might see a 10% rise in 2018

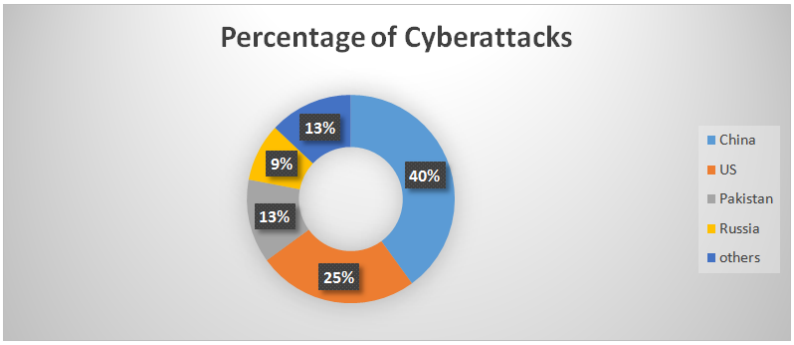

Figure 1: Origin of cyber attacks from January- May 2018

Common Targets

- This year, one in every five cases targeted financial networks.
- Government departments or units too, are becoming targets.
- Power planta, oil refineries oil and gas pipelines in the list.
- Hackers also target telecom and defense communication networks.

- Proportion of attacks on financial networks seeing an increase
- Attacks from Pakistan, North Korea have increased this year.
- An expert says just 5% of cyberattacks reported to authorities
- *Total number of cases in 2018 so far has not been available.*

REVIEW OF LITERATURE

There has been a research done on measuring the attitudes of people to watch their love for money conducted by bank and get you into thousand three and it was found that the concept of love of money construct is ideally related in individuals Their income and proportional to their unethical behavior. This greed for money has been found to be the cause of evil and farther the people with that I would very high income in Hong Kong in generally the service class employees have found to be having a low-level of this money construct are the love for money and this signified that the money construct and income are inversely Proportional to each other. This would mean that those employees who have a lawyer desire for money have a higher satisfaction in their big grades and hands it is very much less likely for them to engage in such unethical behaviors which are related to frogs and scams in the organization's where as the employees and workers which are in the high income grade and status in Hong Kong are suitable he seem to be More engaged in these unethical behaviors and prone to cheat and perform other unethical tasks. This is called the love of money scale and it has been found as one of the most crucial very able which suggests that the employees want to be rich and hence various theories that have been coded upon the satisfaction by the bay of the employee are the equity theory's and that describe band Theories discrete fancy theories it was also tried to find out what are the factors because of which this comparison happens and hands it is a result of the social group comparison with relation to the restaurant as in the circle in which the people move in another study conducted by AW And wrong in 2008 it was farther emphasize that an employee's job pay and output racial has a certain reference and they didn't which would mean that is the ratio of the door is quite similar to what are the reference and dated and then that employee should be satisfied with his or her be. In this case the jury of discrepancy and equity theory also applies true hear the discrepancy theory proves that the perception and attitude of all employees is a discrepant because of The level of satisfaction they draw from their big hands one can receive high satisfaction in less be an ass compared to DC some other restaurant who is in the vice versa situation some other researchers like Sweeney and Mac Farland in 2004 talked about social comparison to our year and a stab list A well-known model in order to predict what is the satisfaction level of employees with the work outcomes it it is related to and satisfaction from work including the pay they get depends on the absolute ruler do comparisons with other people in this circle. The researchers claimed that the comparison Between such salaries and outcomes become very important predictors of job and pay satisfaction. Farther far Lynn in 2005 took the research findings to the level where the comparisons between the similar grade employees were done and more factors which are crucial to their work and be satisfaction of a found out. In order to look beyond comparisons that the famous Researchers sharpie roll and of Abba in 1998 said that the best similar employees which means the other employees working in the same company and doing the same job can also feel least satisfied if they are compared as being reversed or verse performers to Some other colleague in the circle inside or even outside the organization. Hence it became very important that in case of corporate crimes this social status comparison is a very strong determinant which is able to explain the relationship between employee satisfaction bay and gives the highest radiance. Vava Vahala bar farther compared to some of the chosen employees input in the work to the outcome and the ratio between the two with similar rank employees and found that relatively it is in a good table because the first Employee

in his perception remains dissatisfied with the baby and the other one remains happy and satisfied. This became a very well excepted model to predict the employees relationship towards the organization and financial organization their satisfaction with the work they are paying rent and how much of a relative comparable comparison culture exists In their social group in the company. It has been found naturally that people are motivated to compare with their similar counterparts because they want to obtain information which they can relate and find relevant to their own self, as mentioned by Sweeney in 2006. According to PwC's Global Survey 2014, among all the respondents the firm interviewed, one-fourth had been the prey of some formof economic fraud perpetrated by cybercrime, and one-tenth had suffered losses of more than $ 1 million. Furthermore, almost half of those who had been victimized by economic crime felt that the risk of cybercrime is growing significantly. The CEO of the giant American retailer Target had to resign in May 2014 due to the misdeeds of online intruders stealing 40 million of company's digital customers' records. Once they penetrated Target's computer system, the cyber criminals installed malware on its point-of-sale tills to capture the debit and credit card details of the company's customers. Hackers and extractors use different techniques and languages to scare users and extract money. In the USA, messages were said to be purportedly sent by the FBI; in the Netherlands from the local police and so on. Some computer users were gullible and paid the so-called fine only to find that it was a scam. Demanding money for not leaking proprietary information of victims on the Internet is a new tactic to make a fast buck used by extortionist hackers. Hackers are also attacking websites for activist purposes. In 2011, they attacked PayPal in retaliation to its blocking donations to Wiki leaks. They also attacked the websites of the FBI, the Motion Picture Association of America (MPAA) and others to protest against proposed anti-piracy legislation. Extortion is an evil art, which cyber fraudsters seem to have mastered. In early 2012, hackers threatened Symantec that they would post the source code of its popular pc Anywhere antivirus software. They sent it an extortion notice which stated that they would not release the company's source code if they were given ransom money. The hackers called themselves 'Lords of Dharmaraja' and posted 1.3 gigabytes of Symantec's source code on a file-sharing site. It was distributed hundreds of times in a day after posting the extortion notice to the company. Symantec had identified 16 ransom ware gangs and tracked one such gang, which tried to infect more than 500,000 computers just over a fortnight. Moreover, the hackers claimed that they had discovered Symantec's source code when they hacked India's military and intelligence servers in January 2012.The hackers revealed that Symantec offered them money for not releasing further source codes. They however continued to ask for money, and when Symantec did not agree to this, they posted more codes. At one time, they gave 10 minutes time to Symantec to remit $50,000 to an offshore Liberty Reserve account, and when the company asked for more time, they posted some more source codes. Symantec reported that it has prepared itself for any eventuality relating to the rest of its source codes being posted for public consumption by the hackers. In January 2013, The New York Times suffered due to cyber-attacks and suspected spear phishing through emails to its employees. Spear phishing is an art—a message could seem to come from a colleague down the corridor, complete with the appropriate jargon, official language or acronyms usually used. It is very difficult to sift the chaff from the grain. A huge financial fraud (based on phishing) was unearthed through Operation Phish Phry, which was carried out by the FBI in the USA in 2009. The victims had accounts in the Bank of America and Wells Fargo. The fraudsters tricked people into providing their personal banking information and stole around $2 million during 2007-09. The fraud was planned in Egypt, from where mass mails were sent that looked like authentic communication from banks. Whoever clicked on these email messages was directed to fake identical looking bank sites, where they were asked to enter personal information details pertaining to their bank accounts as well as their social security numbers and driving licenses. Based on this information, fraudsters in the USA transferred funds to their own accounts and remitted some to their

accomplices in Egypt. In early 2011, a massive security breach took place where names and email addresses were stolen from a marketing firm, Epsilon, a unit of Alliance Data. The victims were customers of big names such as JP Morgan, Citibank, Target, Barclays, US Bancorp, Walt Disney, Ritz-Carlton and Best Buy. These sorts of fraudulent activities lead to phishing attacks, wherein emails are made to look as though they are from authentic business partners, but the main purpose of the fraudsters is only to acquire account numbers and other personal details of their victims. Phishing attacks are on the rise. In 2013, $6 billion was lost around the world due to phishing attacks, compared to $1.5 billion in 2012. And according to the RSA Fraud Report published in January 2014, India incurred the highest loss of $225 million among the APAC countries. Even Citibank Can Be Fooled! Cybercrime is an economic offence carried out on computers via the Internet. It involves the use of a large and ever-changing variety of tricks, and includes illegal downloading of files, data theft and loss, distribution of viruses, pharming (redirection of web information to another fraudulent site with a malevolent motive), phishing (theft of personal information such as bank passwords and account details) and computer hacking. Development and progress are accompanied by pain at times. Cybercrime is the latest kind on the block, which has infiltrated the world of fraud world unheralded. And with more and more technological razzmatazz being thrust into our lives, cybercrime is bound to spread out its tentacles more pervasively. Cybercrime is now a major risk, demanding immediate attention for any organisation where Internet is part of their business strategy, thus virtually engulfing every enterprise. All that you and me cannot touch and feel, the cyber scammers can. According to Europol, victims lose a whopping €290 billion ($350 billion) every year due to digital crime around the world. This makes it more profitable than global trade in marijuana, cocaine and heroin combined. An early 2013 study sponsored by Hewlett Packard indicated that companies in the UK and Germany are the victims of at least one successful attack every week. For the moving in the direction of corporate fraud Manning into thousand five's doctor about the concept of opportunity , that is a available because of rich people become attracted to wards greed Finding the loopholes and gaps in the accounting procedures and policies in the public as well as private sector banks this concept was researched and discussed also by tell people know falconer and must deck in 2003 In which they conducted intricate study on the most fraud related activities at VA by the organization's, found out the main dispute in cases of miscalculation Ends and damages, analyzed the gaps in valuations of organization, find out the role of the auditor and the fraud examiner. Into thousand and 12 Ramazzotti Rama Zonnie conducted a huge survey research in order to understand the reasons with respect to accountant and their intentions Find the opportunity of their fraud once they are aware about it in the system. They suggested that if there is continuous and Alice's and monitoring then any fraud can be caught in the nip of the bad Detected and of course prevented well before on time. Best seen 2016 studying on what are the possible solutions to minimize and totally I need the factors and causes of financial fraud's. He suggested that the accounting policy of the organization's should be very well totally examined by different export groups because it would help in reducing any possibility of finding the opportunity to the people To get involved in financial this appropriateness. Coming down do another very important factor do you do which such frogs and scams happen is pressure . Where are your studies have shown that the primary reason of fraud committed by an individual is financial pressure, Kretched in 2007 talked about many forms of frauds and the reasons for the He's as to why any employee comes under pressure and gets to conduct fraudulent activities. It was found that an individual or organization or its employee does or tries to do the frog due to his or her first authority Or job position in that organization, because of individual financial commitments including greed there comes pressure on the person which lowers them To conduct unethical activities in France frauds. Frauds happen because the natural human feeling also fear and guilt due to rationalize Asian Is lost, hands because of his position Bible and pressure he goes towards committing fraud

METHODOLOGY

It simply means the methods which have been applied in completing a research study. Methodology generally includes three aspects – Sampling, Tools of Data Collection, and Tools of Data Analysis. Each one is explained below:

Sampling: The researcher visited five courts in Haryana and Delhi and personally handed over the copies of the structured questionnaire to the available Advocates and Judges with a request

to kindly provide the requisite information as per the questions of the questionnaire. With a great effort and after making several rounds to the respondents, the researcher could collect filled in questionnaires from 81 Judges and 156 advocates.

Tools of Data Collection: A structured questionnaire was prepared, keeping in view of the objectives of the study. The researcher after doing extensive review of literature, identified 14 factors of cyber crimes. The options of answer of a factor was on four-point Likert scale, that is, 1 = Disagree, 2 = Neutral, 3 = Agree, and 4 = Strongly Agree. The information of the background variables was also collected from the respondents. The background variables are: Gender, Age, Marital Status, Education, and Occupation.

Tools of Data Analysis: The filled-in questionnaires were entered in the computer with the excel software, and SPSS was applied to do the statistical analysis. The t-test of two independent samples has been applied and the results are presented in the tables along with Mean and SD of total sample. The inferences of each factor are deliberated alongwith the tables.

Research Design: Single cross-sectional descriptive research design is used. In such research designs, the sample is drawn only once and the data are also collected only once. The background variables are described in detail. The description of the factors pertaining to prevention of cybercrimes are described and discussed in detail.

Data Analysis and Interpretations

Profile of the Respondents

Out of the total sample of 237, female constitutes 23.2 per cent, that is, about one fourth of the sample constitutes females (Table 1). So far as the age is concerned, about half of the respondents are of younger age. It is also found from the table that about 70 per cent respondents are married. Around 60 per cent have qualification as above graduation level. About 34 per cent belong to judiciary profession and rest are the advocates.

Table 1: Characteristics of the Respondents (N =237)

Characteristics	Numbers	Percentage
Gender		
-Male	182	76.8
-Female	55	23.2
Age		
-Less than 35years	118	49.8
-35 + years	119	50.2
Marital Status		
-Married	164	69.2
-Unmarried	73	30.8
Education		
-Graduate	93	39.2
-Post graduate	106	44.7
-Above post Graduation	22	9.3

Table 1 Contd.,		
-Others	16	6.8
Profession		
-Judiciary	81	34.2
-Advocate	156	65.8

It is seen from the above paragraphs and also from the literature reviewed for the study that the internet and growing use of e-communication have accelerated the problems of cyber-crimes or frauds. There may be several reasons for cybercrimes or frauds, but as mentioned above that the researcher has identified 14 such reasons or factors after extensively review of literature. The t-test of two independent samples has been applied on the collected data to assess the difference in the opinion of Judges and Advocates respondents on these factors. The findings of the t-test of 14 factors along with the necessary interpretation are presented below:

Professional Networking

Professional Networking is the way for building connection or communication by certain peoples. Peoples can engage, share or connect with other professionals. The purpose of professional networking is to expand your business, build the network, career improvement. What makes a professional network different from a social network service is that it is mainly focused on the relationship of business nature and career building rather than including personal stuff. By using professional networking sites peoples can easily connect with co-workers, professionals from different locality and field. Businesses are able to keep all of their networks up to date. Having a strong network will help you to build the professional career and get in touch with each of them as well as top companies. It also helps to promote business other than social media channels. Sometimes, the likeminded professional having intention to commit frauds would unite together to do it. Therefore, the professional networking may be used to commit crimes or people may indulge in fraudulent activities. The professional network may lead to cybercrime or fraud was the question answered by the respondents on 4-point scale. The t-test of two independent samples has been applied to assess the difference in the option of Judges and Advocates on this variable. The findings of t-test presented in the Table 2 reveal that the mean value is more in the case of Advocates (Mean = 3.12)as compared to Judges (Mean = 2.48). It shows that the opinion of the advocates on an average is approaching to option 4 (Strongly Agree),whereas in the case of judges, it is nearing option 3 (Agree). The t-value indicates that there is a significant difference in the opinion of Judges and Advocates (t = 4.637, significant at.01 level). It is also clear from the overall mean value that on an average all the respondents agree that Professional Networking may lead to cybercrimes.

Table 2: Comparison of views of Judge and Advocate respondents on Cyber Crimes due to Professional Networking

Type of Respondent	N	Mean	S.D.	t-Value
Judges	81	2.48	1.014	4.637**
Advocates	156	3.12	1.005	
Total	237	2.90	1.051	

***Significant at.01 level*

Mean and Standard Deviation values of Professional Networking variable of two types of respondents and the total sample are also presented in **Figure 1.**

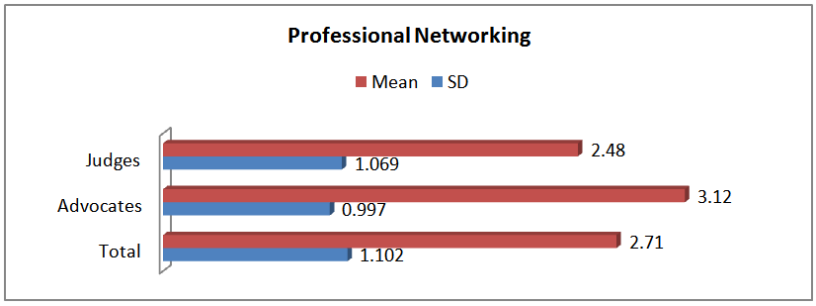

Figure 2

Fake Websites

Criminals create fake websites that look like legitimate websites in order to trick the user into entering their personal information such as their username, password, credit card, or social security numbers. These sites often look identical to the real one and might even have similar web addresses to trick the user. For example, a fictitious fake website (www.bankofamerica1.com) could be made to look like a legitimate bank website (www.bankofamerica.com). Notice the different URLS for the websites. Always type in the URL of the website in an email, do not click on the links. If you are unsure of an email is legitimate always call the business phone number on the website you typed in, not from the email. The information pertaining to Fake Websites that leads to cybercrimes/frauds was gathered from the respondents. The statistical analysis of the same was carried out and the findings are mentioned in the Table 3. It is observed from the Table that the average of responses of Judiciary are around the option 3 (Agree). This simply means that the respondents agree that Fake Websites may lead to crimes or fraudulent activities. On the other hand, on an average the advocates strongly agree that Fake Websites may lead to cybercrimes or fraudulent activities. This is quite evident from the mean value (Mean = 3.21) as it is moving towards the option 4 (Strongly agree). It is further noted from the Table that t-value indicates that there isa significant difference in the opinion of Judiciary and Advocates (t =2.211, significant at.05 level).

Table 3: Comparison of views of Judge and Advocate Respondents on Cyber Crimes due to Fake Websites

Type of Respondent	N	Mean	S.D.	t-Value
Judges	81	2.90	1.032	2.211*
Advocates	156	3.21	.988	
Total	237	3.10	1.012	

***Significant at.05 level*

Mean and Standard Deviation values of Fake Websites variable of two type of respondents are presented graphically in Figure 2:

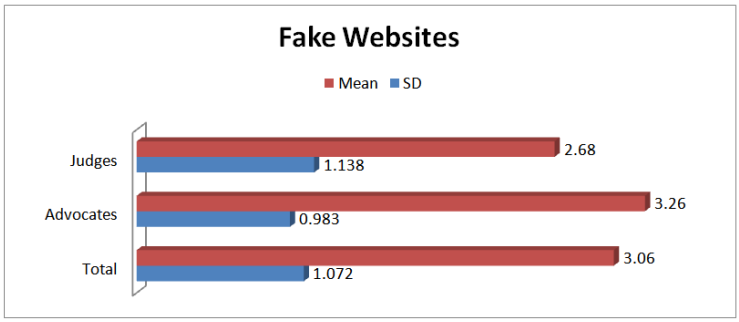

Figure 2

Hacking

Hackingcan also refer to non-malicious activities, usually involving unusual or improvised alterations to equipment or processes.

Hackers employ a variety of techniques for hacking, including:

- Vulnerability scanner: checks computers on networks for known weaknesses
- Password cracking: the process of recovering passwords from data stored or transmitted by computer systems
- Packet sniffer: applications that capture data packets in order to view data and passwords in transit over networks
- Spoofing attack: involves websites which falsify data by mimicking legitimate sites, and they are therefore treated as trusted sites by users or other programs
- Root kit: represents a set of programs which work to subvert control of an operating system from legitimate operators
- Trojan horse: serves as a back door in a computer system to allow an intruder to gain access to the system later
- Viruses: self-replicating programs that spread by inserting copies of themselves into other executable code files or documents
- Key loggers: tools designed to record every keystroke on the affected machine for later retrieval

Certain corporations employ hackers as part of their support staff. These legitimate hackers use their skills to find flaws in the company security system, thus preventing identity theft and other computer-related crimes. The findings of the data collected on this variable from the respondents are presented in Table 4. On an average the Judiciary and Advocates are almost agree in their opinion that the hacking may lead to cybercrimes or fraudulent activities. This is evident from the mean values which are around the option 3 (Agree). Therefore, one has to be quite alert to avoid being trapped in the forged messages that may lead to cybercrimes.

Table 4: Comparison of Views of Judge and Advocate Respondents on Cyber Crimes due to Hacking

Type of Respondent	N	Mean	S.D.	t-Value
Judges	81	2.94	.966	1.602NS
Advocates	156	3.15	.991	
Total	237	3.08	0.986	

NS = Not significant

Mean and Standard Deviation values of Hacking variable of two type of respondents are presented graphically in Figure 3:

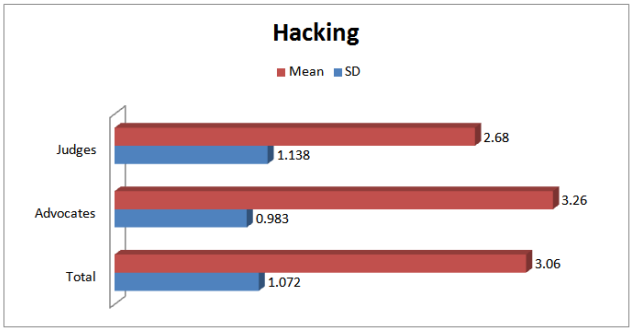

Figure 3

Loose Security Measures

The mean value (Mean = 3.26) of 'Loose Security Measures' is maximum of 'Advocates', whereas it is 2.68 in the case of 'Judiciary'. The difference in mean values is significant as is evident from the t-value (t = 4.060, significant at.01 level). As a matter fact the opinion of the Advocates is moving towards the option 4 (Strongly Agree) while it is approaching option 3 (Agree) in the case of 'Judiciary'. However, the overall mean is 3.06, which indicates that on an average all the respondents agree that Loose Security Measure would result into cybercrimes or fraudulent activities.

Table 5: Comparison of Views of Judge and Advocate Respondents on Cyber Crimes Due to Loose Security Measures

Type of Respondent	N	Mean	S.D.	t-Value
Judges	81	2.68	1.138	4.060**
Advocates	156	3.26	.983	
Total	237	3.06	1.072	

***Significant at.01 level*

Mean and Standard Deviation values of Loose Security Measures variable of two type of respondents are given graphically in Figure 4:

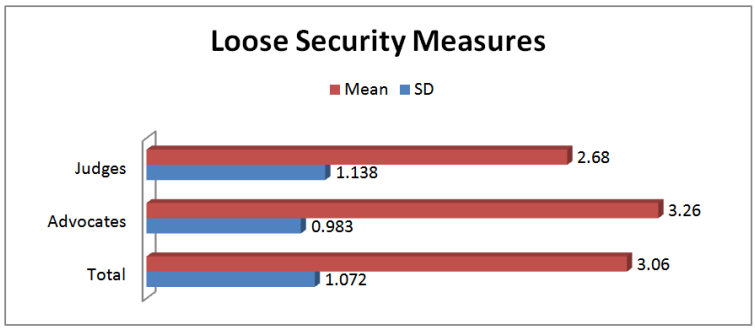

Figure 4

Social Media Sites

Social networking websites are easy to confuse with social media sites. A social networking site is any site that has a public or semi-public profile page, including dating sites, fan sites and so on. A social media site has profiles and connections, combined with the tools to easily share online content of all types. Bad minded persons are using the Social Media Sites for committing cyber-crimes. The respondents were asked to give their opinion to what is extent the social media sites can give way to cybercrimes. The mean value of this variable in the case of 'Advocates' indicates that on an

average (Mean = 3.05) they agree that users of social media sites may commit cyber-crimes, whereas the opinion of the judiciary is around neutral (mean = 2.25). The t-value is significant (t = 5.453, significant at.01 level), it simple means that two types of respondents differ significantly in their opinion, as it is evident from the mean values of this variable.

Table 6: Comparison of Views of Judges and Advocates Respondents on Cyber Crimes Due to Social Media Sites

Type of Respondent	N	Mean	S.D.	t-Value
Judges	81	2.25	1.043	
Advocates	156	3.05	1.094	5.453**
Total	237	2.78	1.141	

***Significant at.01 level*

Mean and Standard Deviation values of Social Media Sites variable of two types of respondents are presented graphically in Figure 5:

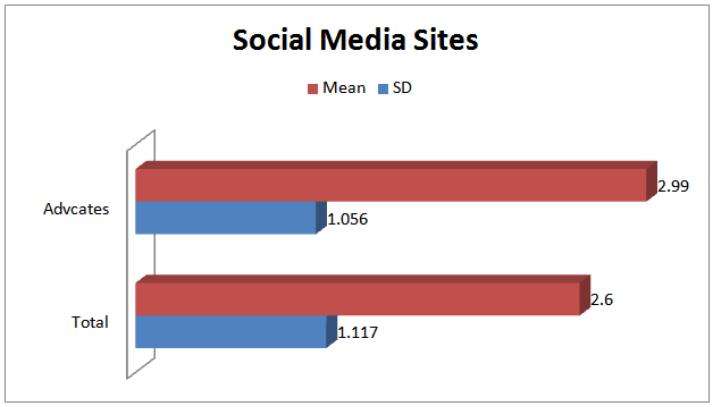

Figure 5

Unsecured Information

If the confidential information of the organization is not secured, any person can have access to that information which could be passed on to other interested persons. This may ultimately lead to crime or fraud. On an average (Mean = 3.09), the advocates categorically agree in their views that unsecured information would lead to cybercrimes/frauds. It is also found from the Table that more or less Judiciary also agree to this (Mean = 2.64). The t-value indicates that the views of two groups differ significantly (t =3.124, significant at.01 level). This is so as the views of advocates are more favourbale to this variable as compared to Judiciary. Further, it is found from the table that on an average all the respondents agree (Mean = 2.94) that if the information in the organization is unsecured that may result into cybercrimes.

Table 7: Comparison of Views of Judges and Advocates Respondents on Cyber Crimes Due to Unsecured Information

Type of Respondent	N	Mean	S.D.	t-Value
Judges	81	2.64	1.121	
Advocates	156	3.09	1.006	3.124**
Total	237	2.94	1.066	

***Significant at.01 level*

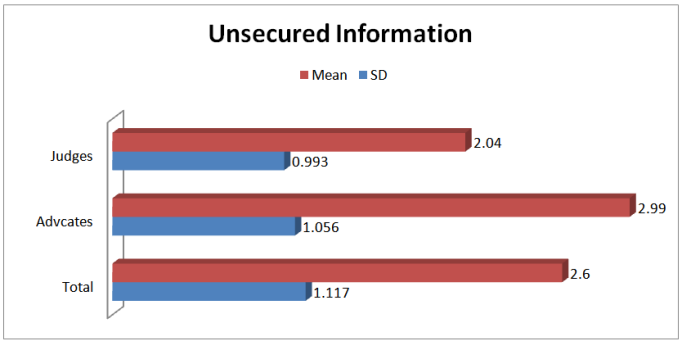

Figure 6

Privacy and Password Settings

A password policy is a set of rules which were created to improve computer security by motivating users to create dependable, secure passwords and then store and utilize them properly. Normally, a password policy is a part of the official regulations of an organization and might be employed as a section of the security awareness training. Although most users understand the nature of security risks related to simple passwords, there is still frustration when users are required to spend time attempting to create a password that meets an unfamiliar criteria or attempting to remember a previously created strong password. **Strong Passwords** are a first line of protection against any unauthorized access into personal computer. The stronger the password, the higher level of protection computer has from malicious software and hackers. A strong password is not just about one password, it is important that you guarantee strong passwords for each account that you access through your computer. When you are utilizing a corporate network, the network administrator may encourage you to use a strong password. If the strong password is not created and kept confidential to oneself, the chances are there that the information kept in the computer would be hacked by the malicious software. This would ultimately lead to crimes/frauds. The findings of this variable in the Table reveal that Advocates on an average (Mean = 2.98) agree that poor privacy and password would give way to crimes/frauds. The mean value (Mean = 2.60) of Judiciary is little less than the option 3 (Agrees). Anyway this mean value is also approaching to the option 3. It may be interpreted that such respondents also agree that poor privacy and password may lead to crimes/frauds.

Table 8: Comparison of Views of Judges and Advocates Respondents on Cyber Crimes due to Privacy and Password Settings

Type of Respondent	N	Mean	S.D.	t-Value
Judges	81	2.60	1.158	2.549**
Advocates	156	2.98	1.032	
Total	237	2.85	1.089	

***Significant at.01 level*

Mean and Standard Deviation values of Privacy and Password Settings variable of two type of respondents are presented graphically in Figure 7:

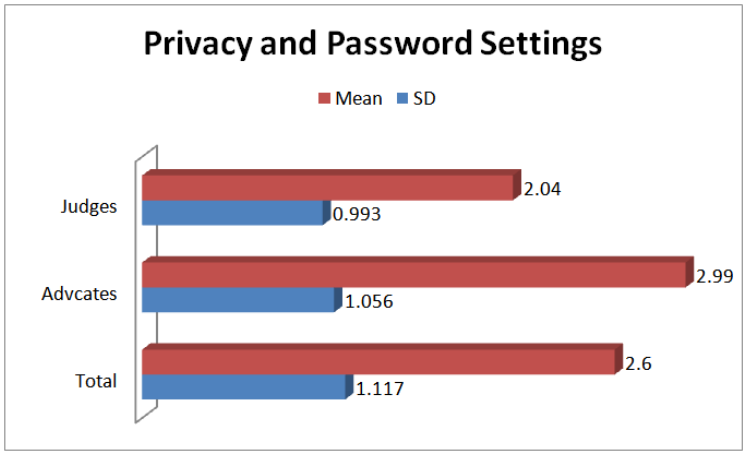

Figure 7

Two-Factor Authentication (2FA)

Two-factor authentication (2FA), sometimes referred to as two-step verification or dual factors authentication, is a security process in which the user provides two different authentication factors to verify themselves to better protect both the user's credentials and the resources the user can access. Two-factor authentication provides a higher level of assurance than authentication methods that depend on single-factor authentication (SFA), in which the user provides only one factor -- typically a password or pass code. Two-factor authentication methods rely on users providing a password as well as a second factor, usually either a security token or a biometric factor like a fingerprint or facial scan. Two-factor (2FA) or multi-factor authentication (MFA) is an additional security layer for business – helping to address the vulnerabilities of a standard password-only approach.

Details of Two Factor Authentication have been explained in the above paragraph. The Table 9 shows that the opinion of the advocates, on an average, are around option 3 (Agree). It shows that on an average they agree that two Factor Authentication would minimize the chances of cyber frauds in the organization. On the other hand the mean value in the case of Judiciary is around option 2 (Neutral), meaning thereby that these respondents neither agree nor disagree that Two Factor Authentication would reduce the chances of cyber crimes. The t-value in the Table is significant which is due to the difference in mean values of two groups (t = 7.202, significant at.01 level).

Table 9: Comparison of views of Judges and Advocates Respondents on Cyber Crimes Due to Two Factor Authentication

Type of Respondent	N	Mean	S.D.	t-Value
Judges	81	2.04	1.030	7.202**
Advocates	156	3.05	1.027	
Total	237	2.70	1.134	

***Significant at.01 level*

Mean Standard Deviation values of Two Factor Authentication variable of two types of respondents and the total sample are presented in Figure 8.\

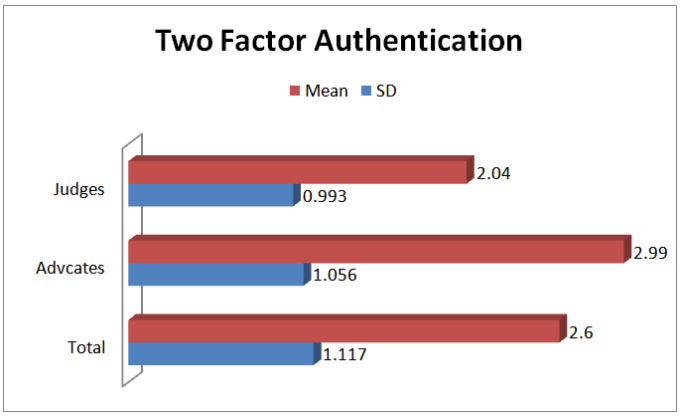

Figure 8

Antivirus Software

Antivirus software is a program or set of programs that are designed to prevent, search for, detect, and remove software viruses, and other malicious software like worms, trojans, adware, and more. These tools are critical for users to have installed and up-to-date because a computer without antivirus software protection will be infected within minutes of connecting to the internet. The bombardment is constant, which means antivirus companies have to update their detection tools regularly to deal with the more than 60,000 new pieces of malware created daily. Today's malware (an umbrella term that encompasses computer viruses) changes appearance quickly to avoid detection by older, definition-based antivirus software. Viruses can be programmed to cause damage to your device, prevent a user from accessing data, or to take control of your computer.

What Does Anti Virus Software Do?

Several different companies build antivirus software and what each offer can vary but all perform some essential functions:

- Scan specific files or directories for any malware or known malicious patterns
- Allow you to schedule scans to automatically run for you
- Allow you to initiate a scan of a particular file or your entire computer, or of a CD or flash drive at any time.
- Remove any malicious code detected –sometimes you will be notified of an infection and asked if you want to clean the file, other programs will automatically do this behind the scenes.
- Show you the 'health' of your computer.

Installation of anti-virus software in the computer may reduce the chances of cyber frauds in the organization. The 'Advocate' respondents have endorsed their opinion to this as the mean value in their case is around option 3 (Agree), whereas the respondents of judiciary are having neutral opinion to this, as is evident from the mean value (Table 10), which is around option 2 (Neutral). The t-value indicates that the respondents of two categories differ in their opinion significantly (t = 7.491, significant at.01 level).

Table 10: Comparison of views of Judges and Advocates Respondents on Cyber Crimes due to Anti-Virus Software

Type of Respondent	N	Mean	S.D.	t-Value
Judges	81	1.93	1.010	
Advocates	156	2.99	1.056	7.491**
Total	237	2.63	1.156	

***Significant at.01 level*

Mean and Standard Deviation values of Anti-virus Software variable of two types of respondents and the total sample are also presented in Figure 9.

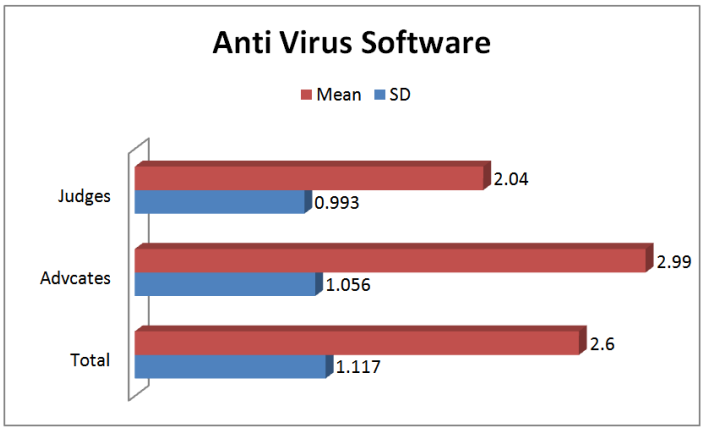

Figure 9

Data Backup

In information technology, a **backup**, or **data backup**, or the process of **backing up**, refers to the copying into an archive file of computer **data** so it may be used to restore the original after a **data** loss event. Or data backup is a process of duplicating data to allow retrieval of the duplicate set after a data loss event. The primary purpose is to recover **data** after its loss, be it by **data** deletion or corruption. Today, there are many kinds of data backup services that help enterprises and organizations ensure that data is secure and that critical information is not lost in a natural disaster, theft situation or other kind of emergency.

The concept of Back-up Data and Information has been explained in the above paragraph. Keeping in view the importance and need of this, it is very much pertinent to have back up of the important data because one never knows when the original data gets corrupted. There may be some people who try to delete or disable the access of company's data set for their personal gains. Therefore, the company should always try to save data in the company. One important method is to keep the back-up of the data or information which is important for the company. The views of the respondents gathered on this have been analyzed and presented in the Table 11. The mean value in the case of Judiciary is around option 2 (Neutral). It may simply means that the respondents of this group neither agree nor disagree in their opinion that keeping Back-up of Data would reduce the cyber-frauds. The Advocates on an average agree that this would reduce the cyber-crimes or frauds (Mean = 2.90). The t-value is 6.021 which is significant at.01 level, this means that two groups differ significantly in their opinion on this variable.

Table 11: Comparison of Views of Judges and Advocates Respondents on Cyber Crimes Due to Back-up of Data and Information

Type of Respondent	N	Mean	S.D.	t-Value
Judges	81	2.04	.993	6.028**
Advocates	156	2.90	1.067	
Total	237	2.60	1.117	

***Significant at.01 level*

Mean Standard Deviation values of Back up of Data and Information variable of two types of respondents and the total sample are also presented in Figure 10.

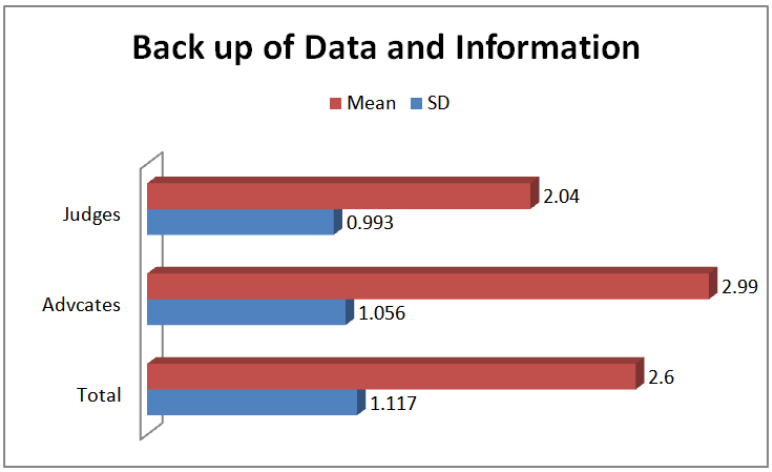

Figure 10

Screen Lock Option

You can help secure your Android phone or tablet by setting a screen lock. Each time you turn on your device or wake up the screen, you will be asked to unlock your device, usually with a PIN, pattern, or password. On some devices, you can unlock with your fingerprint or automatically unlock in trusted conditions. The main purpose of all the measures, which are discussed in this section, is to save the confidential data or information of the company from piracy or misuse or destruction for personal gains by few people. If it is not done, there are chances of frauds or crimes in the company. Screen lock option is one of such measures. The computer screen would only be unlocked by some confidential codes, etc. The opinion collected on this variable from respondents have been given statistical treatment and the findings are presented in Table 11. The judiciary's opinion have minimum mean value (Mean = 1.77). This, of course, is approaching to the option 2 (Neutral), whereas the Advocates on an average agree (Mean = 2.78) that by not protecting the data with Screen Lock Option may lead to cyber crimes/frauds. The t-value in the Table is significant that shows that the respondents of two groups differ significantly in their opinion. This is evident from the mean values of two types of respondents in the Table.

Table 12: Comparison of views of Judges and Advocates respondents on Cyber Crimes due to Screen Lock Option

Type of Respondent	N	Mean	S.D.	t-Value
Judges	81	1.77	.912	7.244**
Advocates	156	2.78	1.069	
Total	237	2.43	1.124	

***Significant at.01 level*

Mean and Standard Deviation values of Screen Lock Option variable of two types of respondents and the total sample are also presented in Figure 11.

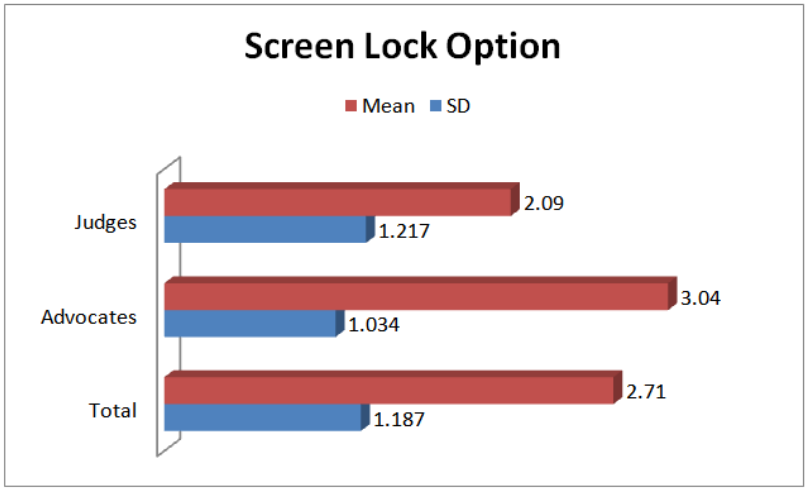

Figure 11

An unsecure Wireless (Wifi) Connection

An unsecure wireless connection is one you can access without a password. Public networks offered in places like cafes are often open. Although these provide free wireless internet access, using public Internet comes with dangers. If your home Internet is open, you should consider securing wireless access to protect your data and avoid legal trouble.

Unsecure Wi-Fi: The two types of public networks are ones that are left open by businesses and ones that are left open by individuals. An open network from a business allows customers to use the Internet in the establishment -- such as patrons of a coffee shop using the network to work. An open network in a home comes from a router that hasn't been secured. Sometimes this is unintentional, if the owner doesn't know that his/her network is open. However, an unsecure wireless connection isn't always bad. Some experienced users opt to leave their Wi-Fi open for the public to access, with proper security precautions to protect their data and bandwidth.

The Risks of Hosting Open Wi-Fi: Although there isa certain nobility in sharing your Wi-Fi with your neighborhood, there's also a danger in it. Unscrupulous users sometimes cruise around looking for unsecure wireless connections to exploit -- such as the 2011 arrest of a man after someone else used his open wireless to download child pornography.

If the wifi connection or internet is not secure in any organization, the probability of cyber crimes or frauds would be more. Therefore, the organization should protect the wifi connection with strong password or pin code. Although, there is difference in mean values of two groups on this variable, but these mean values are approaching to option 3 (Agree). Of course, all the respondents on an average are of the views that unsecure wifi connections would increase the chances of cyber frauds or crimes in the organization. The protection of wifi connections would minimize the chances of cyber crimes or frauds. The t-value is significant (t = 3.931, significant at.01 level). This, of course, shows the extent of variations in the opinion of respondents of two groups.

Table 13: Comparison of Views of Judges and Advocates Respondents on Cyber Crimes due to Unsecure Public WIFI

Type of Respondent	N	Mean	S.D.	t-Value
Judges	81	2.41	1.181	3.931**
Advocates	156	2.99	1.038	
Total	237	2.70	1.122	

***Significant at.01 level*

Mean Standard Deviation values of Unsecred Public Wifi variable of two types of respondents and the total sample are also presented in Figure 12.

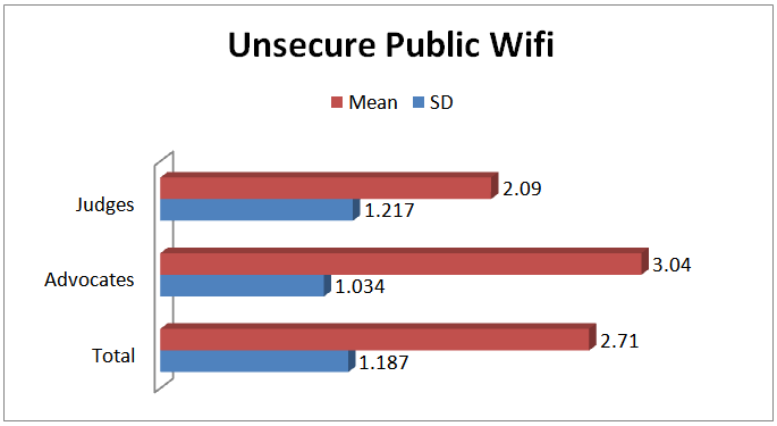

Figure 12

Recognized and Secured Payment Gateway

Simply put a payment gateway is an online equivalent of a card swiping device. If anyone has to accept payments for his physical shop, he uses a card swiping device. Similarly, if one has to accept payments online, they have to use a payment gateway. It is an app that authorizes payments for online businesses through various modes like Net Banking, Credit / Debit Cards and online Wallets. A payment gateway provides a direct connection between a website and a bank, which means that payments can be made directly on your website by end-customers and it gets deposited straight into your current bank account.

In the absence of recognized and secured payment gateway in the company, the chances of cyber crimes or frauds would increase. But according to views of respondents, the opinion of Judiciary is neutral (Mean = 2.09), whereas the opinion of advocates shows that on an average they agree that recognized and secured payment gateway would minimize the chances of cyber crimes or frauds (Mean = 3.04). The difference in the opinion of Judiciary and Advocates is evident from the significant t-value (t = 6.322, significant at.01 level).

Table 14: Comparison of views of Judges and Advocates Respondents on Cyber Crimes due to Recognized and Secured Payment Gateway

Type of Respondent	N	Mean	S.D.	t-Value
Judges	81	2.09	1.217	6.322**
Advocates	156	3.04	1.034	
Total	237	2.71	1.187	

***Significant at.01 level*

Mean and Standard Deviation values of Secured Payment Gateway variable of two types of respondents and the total sample are also presented in Figure 13.

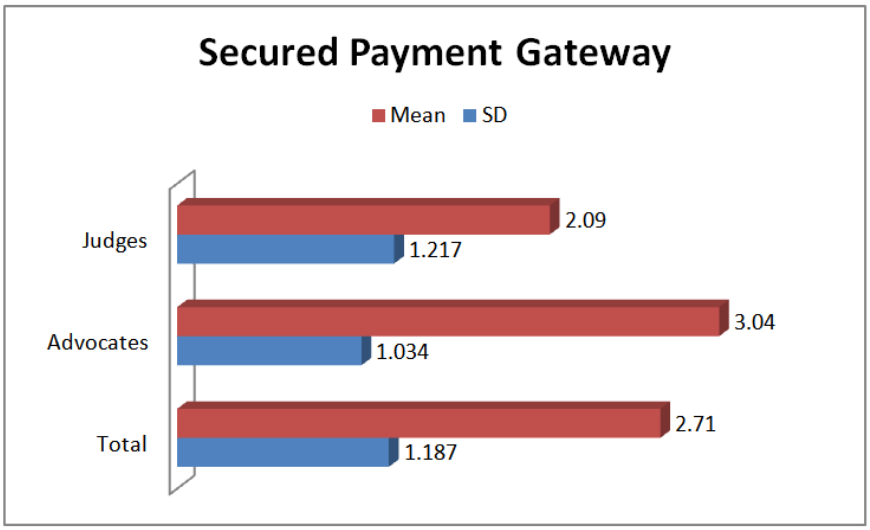

Figure 13

Remote Access to Computer (Connection)

With Remote Desktop Connection, you can connect to a computer running Windows from another computer running Windows that's connected to the same network or to the Internet. For example, you can use all of your work computer's programs, files, and network resources from your home computer, and it's just like you're sitting in front of your computer at work. To connect to a remote computer, that computer must be turned on, it must have a network connection, Remote Desktop must be enabled, you must have network access to the remote computer (this could be through the Internet), and you must have permission to connect. For permission to connect, you must be on the list of users. Before you start a connection, it's a good idea to look up the name of the computer you're connecting to and to make sure Remote Desktop connections are allowed through its firewall. If you're user account doesn't require a password to sign in, you'll need to add a password before you're allowed to start a connection with a remote computer.Remote access to computer (connection) has been explained above. This system may be subjected to various types of cyber crimes or frauds if this is not properly protected with essential measures. The 'Advocates' on an average have expressed their agreement that remote access to computers may increase the chances of cyber frauds or crimes (Mean = 3.01), whereas the opinion of Judiciary is around the option 2 (Neutral). This difference in mean values oftwo groups results into significant difference (t = 6.266, significant at.01 level).

Table 15: Comparison of Views of Judges and Advocates Respondents on Cyber Crimes due to Remote Access to Computer

Type of Respondent	N	Mean	S.D.	t-Value
Judges	81	2.14	1.069	6.266**
Advocates	156	3.01	.997	
Total	237	2.71	1.102	

***Significant at.01 level*

Mean and Standard Deviation values of Remote Access to Computer variable of two types of respondents and the total sample are also presented in Figure 14.

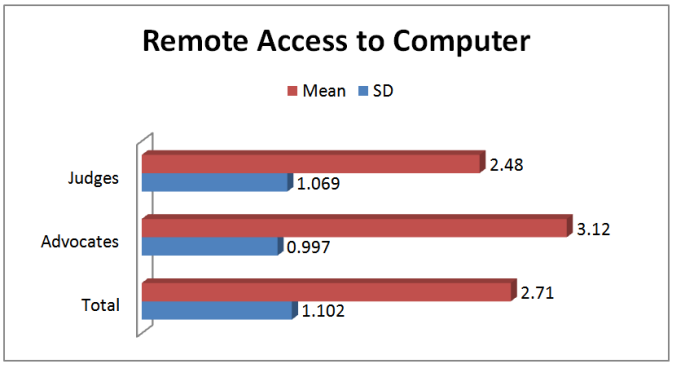

Figure 14

Summary and Conclusions

Cybercrime consists of activities undertaken by an individual or company that are done in a dishonest or illegal manner, and are designed to give an advantage to the perpetrating individual or company. Cybercrime is an economic offence carried out on computers via the internet. It involves the use of a large and ever-changing variety of tricks, and includes illegal downloading of files, data theft and loss, distribution of viruses, pharming (redirection of web information to another fraudulent site with a malevolent motive), phishing (theft of personal information such as bank passbook and accounts details) and computer hacking. Cybercrime is now a major risk, demanding immediate attention for any organization where internet is part of their business strategy, thus engulfing every enterprise. Taking proper or stringent security measures to protect the data and information would prevent cybercrimes. One has to be careful of fake websites and hacking activities.

The opinion of 237 respondents (81 judges and 186 advocates) was collected with the help of structured scale on 14 factors to prevent the cybercrimes. The findings emerged from the study are presented below:

- The respondents on an average are in agreement that Professional networking and Fake Websites are responsible for cybercrimes. One should be cautious about these in order to avoid cybercrimes.
- Hacking is the biggest problem. Almost all the respondents agree that many cybercrimes are taking place only due to hacking. Everyone has to take appropriate measures to avoid hacking of confidential and important information or data.
- Loose security measures and unsecured information would definitely invite the cybercrimes. On an average the respondents agree to this.
- Privacy and Password for accessing the confidential data and information would help in avoiding the cybercrimes.
- The respondents almost in agreement that the **Two Factor Authentication measures would save the data and information from cybercrimes.**
- Anti-virus software would help to combat the cybercrimes provided it is continuously updated.

- Regularly the Back-up of data and information should be stored on a safe media with proper precautions and at safe place. In case of loss of data and information due to cybercrimes, the back could be used.

REFERENCES

1. *Akenbor, C.O. and Ironkwe, U. (2014) Forensic Auditing Techniques and Fraudulent*
2. *Practices of Public Institutions in Nigeria, Journal of Modern Accounting and Auditing, Vol. 10, No. 4, 451-459.*
3. *Albrecht, W. S., Hill, N. C., and Albrecht, C. C. (2006) The ethics development model applied to declining ethics in accounting. Australian Accounting Review, 16(1), 30-40.*
4. *Albrecht, W., Howe, K. and Romney, M. (1984) Deterring fraud: The internal auditor's perspective. Altamonte Springs, FL: The Institute of Internal Auditors ResearchFoundation.*
5. *Asika, N. (2005) Research Methodology in the Behavioural Sciences, Lagos, Longman Nigeria Plc. pp. 27 – 35*
6. *Benartzi, Shlomo and Thaler, Richard H. Naive Diversification Strategies in Retirement Sav-ing Plans. American Economic Review, 2001, 91(1), pp. 79 –98.*
7. *Chao-ying, J. P., Kuk lida l. and Gary, M. I. (2002) An introduction to logistic regression:*
8. *Analysis and Reporting, The Journal of Educational Research, Vol. 96 (No. 1)*
9. *Chi-Chi, O. A. and Ebimobowei, A. (2012) Fraudulent Activities and Financial Accounting services of banks in Port Harcourt, Nigeria, Asian Journal of Business Management 4*
10. *(2): 124-129.*
11. *Costa, P. and McCrae, R. Normal Personality Assessment in Clinical Practice: The NEO Personality Inventory. Psychological As-sessment, 1992, 4(1), pp. 5–13.*
12. *Calderon, T. and Green, B.P. (1994). Internal Fraud Leaves Its Mark: Here's How to Spot, Trace and Prevent It, National Public Accountant, 39(2), August, 17-20.*
13. *Chakraborty, S. (2013). Indian banking set to become fifth largest by 2020: KPMG-CII Report, Business Standard News, September 13, 2013.*
14. *Cotton,M.P. (2000) Corporate Fraud Prevention, Detection and Investigation: A practical*
15. *Guide of Dealing with Corporate Fraud, Australia: Price water house coopers*
16. *Dada, S.O., Owolabi, S.A. and Okwu, A.T. (2013) Forensic accounting a panacea to alleviation of fraudulent practices in Nigeria, International Journal of BusinessManagement and Economic Research, Vol. 4 (5), 787–792.*
17. *Dahli, G. (2008) Forensic Accounting and Auditing: Compared and Contrasted to Traditional Accounting and Auditing, American Journal of Business Education, Vol. 1 No. 2*
18. *Dorminey, J., Fleming, A., Kranacher, M., and Riley, R. (2010) Beyond the fraud triangle.*
19. *The CPA Journal, 80(7), 17-23.*

20. *Eboh, E.C. (2009) Social and Economic Research Principles and Methods, Enugu, African Institute for Applied Economics. pp. 45 - 52*
21. *Enofe, A. O.,Okpako, P.O. and Atube, E.N. (2013) The Impact of Forensic Accounting on Fraud Detection, European Journal of Business and Management ISSN 2222-1905 (Paper) ISSN 2222-2839 (Online) Vol.5, No.26.*
22. *Eyisi, A.S. and Agbaeze, E.K. (2014) The impact of forensic auditors in corporate governance , International journal of Development and Sustainability, Vol. 3 No. 2, pp. 404 – 417.*
23. *Gates, T. and Jacob, K. (2009). Payments Fraud: Perception versus Reality, Economic Perspectives, 33(1), 7-15.*
24. *George, D. and Mallery, P. (2003) SPSS for Windows step by step: A simple guide and*
25. *reference. 11.0 update, Boston: Allyn & Bacon.*
26. *Ghali, M. J. (2001) Fraud awareness auditing, New York, NY, The Dryden Press.*
27. *Grippo, F. J. and Ibex, J. W. (2003) Introduction to forensic accounting, The National Public Accountant, Washington*
28. *Gujarati, D. N. and Porter, D. C. (2009) Basic Econometrics, New York, McGraw-Hill International Edition. pp. 541 - 590.*
29. *Grossberg, S. and Gutowski, W. Neural Dynam-ics of Decision Making under Risk: Affective Balance and Cognitive-Emotional Interac-tions. Psychological Review, 1987, 94(3), pp. 300 –18.*
30. *Hirshleifer, D. and Shumway, T. Good Day Sunshine: Stock Returns and the Weather. Journal of Finance, 2003, 58(3), pp. 1009 – 32.*
31. *International Personality Item Pool. A scientific collaboratory for the development of ad-vanced measures of personality traits and other individual differences. http://ipip.ori. org/.*
32. *Isen, A.; Nygren, T. and Ashby, F. Influence of Positive Affect on the Subjective Utility of Gains and Losses: It Is Just Not Worth the Risk. Journal of Personality and Social Psy-chology, 1988, 55(5), pp. 710 –17.*
33. *Isen, A. and Geva, N. The Influence of Positive Affect on Acceptable Level of Risk: The Person with a Large Canoe Has a Large Worry. Organizational Behavior and Hu-man Decision Processes, 1987, 39(2), pp. 145–54.*
34. *Kamstra, Mark J.; Kramer, Lisa A. and Levi,*
35. *Maurice D. Winter Blues: A SAD Stock Market Cycle. American Economic Review, 2003, 93(1), pp. 324 – 43.*
36. *Krivelyova, A. and Robotti, C. Playing the Field: Geomagnetic Storms and Interna-tional Stock Markets. Federal Reserve Bank of Atlanta Working Paper No. 2003-5a, 2003.*
37. *Kuhlman, D. and Zuckerman, M. Personality and Risk-Taking: Common Biosocial Fac-tors. Journal of Personality, 2000, 68(6), pp. 999 –1029.*
38. *Karwai, M. (2004) Forensic Accounting and Fraud Investigation for Non-Expert, New Jersey: John Wiley and Sons, Inc.*

39. *Kaveri, V.S. (2014). Bank Frauds in India: Emerging Challenges, Journal of Commerce and Management Thought, 5(1), 14-26.*
40. *Lefcourt, H. Locus of Control, in J. P. Robin-son, P. R. Shaver, and L. S. Wrightsman, eds., Measures of personality and social psy-chology attitudes. San Diego, CA: Academic Press, 1991, pp. 413–99.*
41. *Lo, A. and Repin, D. The Psychophysiology of Real-Time Financial Risk Processing. Jour-nal of Cognitive Neuroscience, 2002, 14(3), pp. 323–39.*
42. *Lo, A.; Repin, D. and Steenbarger, B. Fear and Greed in Financial Markets: A Clinical Study of Day-Traders. MIT Laboratory for Finan-cial Engineering Working Paper No. LFE– 1060 – 05, 2005.*
43. *Loewenstein, G. Emotions in Economic Theory and Economic Behavior. American Eco-nomic Review, 2000 (Papers and Proceed-ings), 90(2), pp. 426 –32.*
44. *nizational Behavior and Human Decision Processes, 1998, 76(3), pp. 298 –324.*
45. *Mahdi, S. and Zhila, A. (2008) Fraud detection and audit expectation gap: Empirical from*
46. *Iranian bankers. International journal of business and management, 3(10): 65-67.*
47. *Malphrus, S. (2009), Perspectives on Retail Payments Fraud , Economic Perspectives, 33(1), 31-36.*
48. *Matthews, G.; Jones, D. and Chamberlain, G.*
49. *Refining the Measurement of Mood: The UWIST Mood Adjective Checklist. British Journal of Psychology, 1990, 81(1), pp. 17– 42.*
50. *McCrae, R. and Costa, P. Toward a New Gen-eration of Personality Theories: Theoretical Contexts for the Five-Factor Model, in J. S. Wiggins, ed., The five-factor model of per-sonality: Theoretical perspectives. New York: Guilford, pp. 51– 87.*
51. *Masango, C. (1998) Criminal law manual, Zimbabwe Republic Police Printers, Harare, Zimbabwe.*
52. *Mohd, S. I. and Mazni, A. (2008) An overview of forensic accounting in Malaysia, Kuala Lumpur, University of Malaysia Press Inc.*
53. *Nwankwo, G.O. (1992) Banking Fraud. Lecture delivered at the 5th Anniversary of Money market Association of Nigeria.*
54. *Nwaze, C. (2008) Quality and internal control challenges in contemporary Nigeria banking.*
55. *Zenith economic quarterly, Zenith bank plc, 3(2): 21-32.*
56. *Ofiafoh, E. and Otalor, J.O. (2013) Forensic accounting as a tool for fighting financial crime in Nigeria, Research Journal of Finance and Accounting, Vol. 4, No. 6.*
57. *Okolie, A. and Taiwo, A. (2014) The application of information technology to forensic investigations in Nigeria. Department of Accounting, Ambrose Alli University, Ekpoma, Nigeria.*

58. *Owolabi, S.A. (2010) Fraud and Fraudulent Practices in Nigeria Banking Industry. AnInternational Multi-Disciplinary Journal, Ethiopia. Vol. 4 (3b)*
59. *Pan, S. (2015). An Overview of Indian Banking Industry, International Journal of Management and Social Science Research, Vol. 4, No. 5, May, 67-71.*
60. *Performance of Banks in Nigeria, British Journal of Arts and Social Sciences, 15(1), 12-25.*
61. *Deloitte Fraud Survey (2015), The Deloitte India Banking Fraud Survey Report Edition II. Available at www.deloittee.com/in.*
62. *Pasricha, P. and Mehrotra, S. (2014). Electronic Crime in Indian Banking, Sai Om Journal of Commerce and Management, 1(11), November.*
63. *Rae, K., and Subramaniam, N. (2008) Quality of internal control procedures: Antecedents and moderating effect on organisational justice and employee fraud. ManagerialAuditing Journal, 23(2), 104-124.*
64. *Singleton, J., Singleton, A. T. and Balogna, G. J. (2006) Fraud auditing and forensicaccounting, London, McGraw-Hill.*
65. *Singh, M.K. (2005). Bank Frauds— What Every Banker Needs to Know, IBA Bulletin, September, 3-7.*
66. *Soni, R.R. and Soni, N. (2013). An Investigative Study of Banking Cyber*
67. *Frauds with Special Reference to Private and Public Sector Banks, Research Journal of Management Sciences, 2(7), 22-27 July.*
68. *Soyemi, K.A. (2014) Auditing and Assurance services, Abeokuta, LekSilicon publishing company limited.*
69. *Thaler, R. and Johnson, E. Gambling with the House Money and Trying to Break Even: The Effect of Prior Outcomes on Risky Choice. Management Science, 1990, 36(6), pp. 643– 60.*
70. *Thornhill, W. T. (1995) Forensic accounting, How to investigate financial fraud, New York, NY, Irwin Professional publishing*
71. *Williams, I. (2005) Corrupt practices: Implications for Economic Growth and Development of Nigeria, The Nigeria accountants, 38 (4), pp. 44-50.*
72. *Wolf, D.T. and Hermanson, D.R. (2004) The fraud diamond: considering the four elements of fraud, The certified public Accountants journal*
73. *Yio, G.A. and Cheng, H.P. (2004) Financial crime – what impact has it on Kenya's Economy, International Journal of Economic Development, 12 (3), 89 – 102.*
74. *Zachariah P., Masoyi, A. D., Ernest, E. I.and Gabriel, A.O. (2014) Application of Forensic Auditing in Reducing Fraud Cases in Nigeria Money Deposit Banks,*