A study of White Collar Crime & Cyber Crime (WC2 & C2)

Ms.Sonali B Singhvi
Student B.Com VI SEM Fatima Degree college.
Keshawapur Hubli-580029 Karnataka
sonali.singhvi23@gmail.com

Abstract--In this paper, we examine about the white collar crime & cyber crime mainly focusing in India. White-collar crime refers to financially motivated nonviolent crime committed by business and government professionals. White collar crimes are criminal acts that are performed by people in the course of business committed for financial gain. These types of crimes can cost citizens millions of dollars! These crimes are difficult to prosecute because they often involve sophisticated systems and even many decent people. Cybercrime is a fast-growing area of crime. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual, cause serious harm and pose very real threats to victims worldwide.

A white-collar crime therefore overlaps with corporate crime and cyber crime. The internet in India is growing rapidly. It has given rise to new opportunities in every field we can think of be it entertainment, business, sports or education. There are two sides to a coin. Internet also has its own disadvantages. One of the major disadvantages is Cyber crime illegal activity committed on the internet. The internet, along with its advantages, has also exposed us to security risks that come with connecting to a large network. Computers today are being misused for illegal activities like e-mail espionage, spam, software piracy and so on, which invade our privacy and offend our senses.

It is a saying that: "The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".

Keywords-- White Collar Crime, Other crimes, Cyber Crime, SEBI regulation, eradication & Cyber Law.

I. INTRODUCTION

White collar crime is the illegal activities of people and organizations whose acknowledged purpose is profit through legitimate business enterprise. It is the crime committed by persons of relatively high social or economic status in connection with their regular occupations. White-collar crimes fall broadly into two categories: those illegal actions undertaken by perpetrators to make money for themselves; and those illegal actions undertaken principally to further the aims of their company or other organization. White collar crime involves illegal business practices (embezzlement, price-fixing, bribery) with merchandise that is ordinarily seen as a legitimate business product.

Cyber Crimes The term cyber crime is a broad term that is usually applied to a broad range of crimes in which computers are, in some manner, involved. This term, however, is vague and actually refers to a collection of dissimilar forms of criminal conduct that are powered by different motives. Every computer system is threatened by the large number of crimes which we usually call cyber crimes, but every computer system does not face an equal risk of being victimized by all of those crimes. Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime. As Internet usage continues to rise throughout the world, the threat of cyber crime also grows. While some of these crimes are relatively harmless and commonplace, others are very serious and carry with them felony charges.

II. WHITE COLLAR CRIME-WC2

WC2 IN INDIA

India also recognizes securities frauds as white collar crimes, considering the nature of the crime, class of the offenders involved and the social and economic impact of the crime. However, until date, India has not been able to establish precedents of successful enforcement of insider trading cases that can act as a deterrent against potential violators. India had framed the Insider Regulations way back in 1992. However, in India, there has not been a single case of conclusive conviction of an insider for the violation of the Insider Regulations by the SEBI.

White-collar crimes affected the nation and the society, which was not very much concerned about, as people are not directly affected by the white collar crimes which included, internet hacking, defrauding of banks, printing of counterfeit notes. There is black money of thousands of crores in circulation and criminals are merely escaping with a fine of few thousand rupees for the offences running to several hundred crores. Only four per cent of the white criminals got convicted at the Supreme Court.

III. REASONS FOR WC2

A few reasons common to all jurisdictions including India for non effective prosecution of the white collar crimes are discussed below:

a. Social status: One of the foremost reasons for the ineffective enforcement against white collar crimes is the class of persons involved in the crime. The white collar crimes are usually committed by people with high social status. These offenders have the social, political and economic power to influence such charges against them.

b. Complexity: The perpetrators of the white collar crimes learn the techniques of defrauding and embezzling funds and are aware of the methods to cover up their illegal actions, and therefore, it is very difficult to obtain cogent evidences to prosecute them in court of law. Insider trading is a typical example where collating the evidence against the violator is extremely cumbersome.

c. Corruption: Rampant corruption in the society which makes it possible for the offenders to bribe their way out even when a tribunal or a court finds an individual guilty of white collar crime also is a negating factor for effective enforcement against white collar crimes.

d. Chain Linking: The offence of insider trading involves strong ties among the individuals who commit crimes. The offence is committed by the professionals as a group and are mostly of high social status who have knowledge, techniques and tactics to undertake such crimes, besides that they employ strategic means of acquiring funds and opportunity, which makes it difficult to trace the suspect and prosecute.

Relationship to other types of crime

a. Blue-collar crime: Blue-collar crime tends to be more obvious and thus attracts more active police attention such as vandalism or shoplifting. In contrast, white-collar employees can incorporate legitimate and criminal behavior, thus making themselves less obvious when committing the crime. Therefore, blue-collar crime will more often use physical force, whereas in the corporate world, the identification of a victim is less obvious and the issue of reporting is complicated by a culture of commercial confidentiality to protect shareholder value. It is estimated that a great deal of white-collar crime is undetected or, if detected, it is not reported.

b. Corporate crime: Corporate crime deals with the company as a whole. The crime benefits the investors or the individuals who are in high positions in the company or corporation. The relationship white-collar crime has with corporate crime is that they are similar because they both are involved within the business world. Their difference is that white-collar crime benefits the individual involved, and corporate crime benefits the company or the corporation.

c. State-corporate crime: The negotiation of agreements between a state and a corporation will be at a relatively senior level on both sides; this is almost exclusively a white-collar "situation" which offers the opportunity for crime. Although law enforcement claims to have prioritized white-collar crime, evidence shows that it continues to be a low priority. When senior levels of a corporation engage in criminal activity using the company this is sometimes called control fraud.

d. Organized transnational crime: Organized transnational crime is organized criminal activity that takes place across national jurisdictions, and with advances in transportation and information technology, law enforcement officials and policy makers have needed to respond to this form of crime on a global scale. Some examples include human trafficking, money laundering, drug smuggling, illegal arms dealing, terrorism, and cybercrime.

e. Occupational crime: Individuals may commit crime during employment or unemployment. The two most common forms are theft and fraud. Theft can be of varying degrees, from a pencil to furnishings to a car. Insider trading, the trading of stock by someone with access to publicly unavailable information, is a type of fraud.

IV. CYBER CRIME- C2

C2 in India

The rate at which cyber crime in India is growing is very alarming. The statistics on cyber crime in India paint a picture that none can be proud of. The only hope ahead is that the Union Government has cleared the setting up of the National Cyber Crime Coordination Centre. The setting up of the NCCC was pending since 2013 and it was only last month that the finance ministry gave the nod to set up the centre at an estimated cost of Rs 800 crore.

A detailed report was prepared by The Associated Chambers of Commerce & Industry of India in which it stated that the number of cyber crimes in India may touch a humungous figure of 3, 00,000 in 2015, almost double the level of last year. While releasing the joint study on "Cyber and Network Security Framework" D S Rawat, Secretary General ASSOCHAM said, "What is causing even more concern is that the origin of these crimes is widely based abroad in countries including China, Pakistan, Bangladesh and Algeria among others".

Reasons for C2

Hart in his work □The Concept of Law□ has said □human beings are vulnerable so rule of law is required to protect them□. Applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cyber crime. The reasons for the vulnerability of computers may be said to be:

1. Capacity to store data in comparatively small space.
2. Easy to access.
3. Complex.
4. Negligence.
5. Loss of evidence.

V. MEASURES TO CURB C2

Prominent measures

A) Encryption: This is considered as an important tool for protecting data in transit. Plain text (readable) can be converted to cipher text (coded language) by this method and the recipient of the data can decrypt it by converting it into plain text again by using private key. This way except for the recipient whose possessor of private key to decrypt the data, no one can gain access to the sensitive information.

B) Synchronized Passwords: These passwords are schemes, used to change the password at user□s and host token. The password on synchronized card changes every 30-60 seconds which only makes it valid for one time log-on session. Other useful methods introduced are signature, voice, fingerprint identification or retinal and biometric recognition etc. to impute passwords and pass phrases

C) Firewalls: It creates wall between the system and possible intruders to protect the classified documents from being leaked or accessed. It would only let the data to flow in the computer which is recognized and verified by one□s system. It only permits access to the system to ones already registered with the computer.

D) Digital Signature: These are created by using means of cryptography by applying algorithms. This has its prominent use in the business of banking where customer□s signature is identified by using this method before banks enter into huge transactions.

Preventive measures

1. To prevent cyber stalking, avoid disclosing any information pertaining to one self.
2. Always avoid sending photographs online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
3. Always use latest and update antivirus software to guard against virus attacks.
4. Always keep back up volumes so that one may not suffer data loss in case of virus contamination
5. Never send your credit card number to any site that is not secured, to guard against frauds.
6. Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
7. It is better to use a security program that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
8. The web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
9. Use of firewalls may be beneficial.
10. Web servers running public sites must be physically separate and protected from internal corporate network.

Cyber Laws

Cyber crimes are a new class of crimes which are increasing day by day due to extensive use of internet these days. To combat the crimes related to internet The Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take in to its purview cybercrimes.

The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

1 Cybercrimes under the IT Act:

*Tampering with Computer source documents-Sec.65
*Hacking with Computer systems, Data alteration-Sec.66
*Publishing obscene information-Sec.67
*Un-authorized access to protected system Sec.70
*Breach of Confidentiality and Privacy-Sec.72
*Publishing false digital signature certificates-Sec.73

2 Cyber Crimes under IPC and Special Laws:

*Sending threatening messages by email-Sec503IPC
*Sending defamatory messages by email-Sec499IPC
*Forgery of electronic records-Sec463IPC
*Bogus websites, cyberfrauds-Sec420IPC
*Email spoofing-Sec463IPC
*Web-Jacking-Sec.383IPC
*E-Mail Abuse-Sec.500IPC

3 Cyber Crimes under the Special Acts:

*Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act *Online sale of Arms and Arms Act

VI. LINK BETWEEN WC2 AND C2

The latest developments in information technology and electronic media especially during 1990's have given rise to a new variety of computer related white collar crime which is commonly called cyber crimes. The widespread growth of these crimes has become a matter of global concern and a challenge for the law enforcement agencies in the new millennium. Because of the peculiar nature of these crimes, they can be committed anonymously and far away from the victim; without being physically present there. Further, cyber criminals have a major advantage; they can use computer technology to inflict damage without the risk of being caught. The cyber crimes cover a wide range of illegal computer related activities which include offences such as theft of communication services, industrial espionage, dissemination of pornographic and sexually offensive material in cyber space, electronic money laundering and tax evasion, electronic vandalism, terrorism and extortion, telemarketing frauds, illegal interception of telecommunication etc.

Besides virus, there are some common cyber offences which are directed, against computer systems, networks or data. Notable among them are:

(1) Pheakering: It is a way to circumvent the billing mechanism of telephones allowing anyone to call anywhere in the world literally without any cost.

(2) Internet frauds: Cyber space now provides a wide variety of investment opportunities opening new areas for deceit or, fraud. Electronic funds transfer systems have begun to proliferate, hence there is risk of

transactions being intercepted or diverted. Now a days valid credit card numbers can be intercepted electronically as well as physically and the digital information stored on a card can be counterfeited.

(3) Hackers: Hacker is one, who enjoys ex programmable systems and knows, how to strelet their capacity, computer hackers may affect the commercial websites or e mail systems thus paralyzing the entire business.

(4) Stalking: In stalking, persistent messages are sent to unwilling recipients thus causing them annoyance, worry and mental torture.

(5) E mail security invasion: It means to encrypt the E mail and, make it private and non viewable to others.

(6) Money Laundering: It is a kind of cyber crime in which money is illegally down loaded in transit.

(7) Data Diddling: It mean's changing or erasing of data in subtle ways which makes it difficult to put the data back or be certain of its accuracy.

VII. CONCLUSION

I would like to say that if everyone at a particular business or company would keep an eye out for anything suspicious that alone would detour potential thieves. The real solution to this problem is going to have to come from the people who are being affected by it. They are the most likely to stop it. They cannot let anyone take advantage of them anymore. Most do not give white collar crimes much thought because they are only things that they read about in newspapers and hear on the news. If these crimes continue to grow at the present rate, they will be out of control before we know it.

The regulatory framework in India should treat insider trading as a grave white collar crime and insert provisions in the SEBI Act itself prescribing this as a crime, followed by the consequence of imprisonment. Currently there is no separate provision for penal consequences for the offence of insider trading. Section 24 of the SEBI Act provides for criminal prosecution if any person contravenes any of the provisions of the Act or rules or regulation made under the Act and could result in a punishment up to an imprisonment of ten years with or without fine which may extend to Rs.20 crores. This provision for criminal prosecution is not specific to the enforcement of insider trading laws alone. As stated above, there is not a single reported case of successful prosecution of insider trading.

It□s like □eye for an eye□ kind of situation where the technology can be curbed only by an understanding of the technology taken over by cyber terrorists. Even if the technology is made better enough to curb the computer related crime there is no guarantee if that would stay out of reach of cyber terrorists. Therefore Nations need to update the Law whether by amendments or by adopting sui generic system.

VIII. REFERENCES

[1].https://en.m.wikipedia.org/wiki/White-collar_crime
[2]. http://www.abc-clio.com/ABC-CLIOCorporate/product.aspx?pc=A2212C
[3].http://www.acfe.com/products.aspx?id=2296
[4].http://indianresearchjournals.com/pdf/IJSSIR/2012/September/16.pdf
[5].http://study.com/academy/lesson/what-is-white-collar-crime-definition-statistics-examples.html
[6].http://www.legalservicesindia.com/article/article/white-collar-crime-and-its-changing-dimensions-in-india-1378-1.html
[7].http://www.publishyourarticles.net/knowledge-hub/essay/essay-on-white-collar-crimes-in-india/4900/
(((http://juris.nationalparalegal.edu/(X(1)S(jczxrhh1kom0cabtvbpprfhs))/WhiteCollar.aspx
[8].http://www.amicus.iupindia.org/WhiteCollarCrimes_ovw.asp
[9].http://www.legalserviceindia.com/articles/article 2302682a.htm
[10].http://www.123oye.com/job-articles/cyber-law/phising.htm Information Technology Act, 2000
[11].http://www.google.co.in/url?q=http://googleweblight.com/%3Flite_url%3Dhttp://www.legalservicesindia.com/article/article/white-collar-crimes-cyber-crimes-255-1.html%26ei%3DCyPb_B_u%26lc%3Den-IN%26geid%3D10%26s%3D1%26m%3D732%26ts%3D1454166047%26sig%3DALL1Aj7mgio-N5Aa7Oh3Vu7pCq-fTYef5Q&sa=U&ved=0ahUKEwie4ZrV5tHKAhVHGI4KHVOhBCQQFgggMAU&usg=AFQjCNEWvwwH5G8OeWUlezGgKETjoizjNg
[12].http://www.google.co.in/url?q=https://www.linkedin.com/pulse/20140813191900-273389505-criminology-white-collar-crimes-in-india%3FforceNoSplash%3Dtrue&sa=U&ved=0ahUKEwj1gNrn5tHKAhXIj44KHekdA0YQFggXMAI&usg=AFQjCNHfM9xz6lLhwDQKXb_35OqcL9UEAA
[13].http://www.google.co.in/url?q=http://m.timesofindia.com/home/sunday-times/deep-focus/When-crime-gets-creative/articleshow/4653226.cms&sa=U&ved=0ahUKEwiKkamK59HKAhVIj44KHfmqBFUQFggjMAU&usg=AFQjCNEN--2gayGVKudrS4iLllmZfh1q5A
[14].http://www.google.co.in/url?q=http://googleweblight.com/%3Flite_url%3Dhttp://www.cyberlawsindia.net/internet-crime.html%26ei%3DsVCF56Vy%26lc%3Den-IN%26geid%3D10%26s%3D1%26m%3D732%26ts%3D1454167997%26sig%3DALL1Aj47z8FQCL18fcKYbs5m5nDxLyql2w&sa=U&ved=0ahUKEwjQmKT37dHKAhWF6KYKHWT3AX4QFggRMAA&usg=AFQjCNEvWEMev2pi1Kfjv6aevSZVHmsExg

[15].http://googleweblight.com/?lite_url=http://lawprojectsforfree.blogspot.com/2010/09/crimionology-white-collar-crimes-in.html?m%3D1&ei=xaDh0xt7&lc=en-IN&geid=10&s=1&m=732&ts=1454211873&sig=ALL1Aj6O6aelilVUjfQHq1SMDcOiJjbRLQ
[16].http://googleweblight.com/?lite_url=http://www.helplinelaw.com/employment criminal-and-labour/CCII/cyber-crimes-in-india.html&ei=NbePk-k_&lc=en-IN&geid=10&s=1&m=732&ts=1454229336&sig=ALL1Aj5sYP9DAusGc44bR1BBrWhCcrkdtA
[17].http://www.oneindia.com/feature/cyber-crime-rising-is-india-doing-enough-1882982.html
[18].https://www.linkedin.com/pulse/20140813191900-273389505-criminology-white-collar-crimes-in-india?forceNoSplash=true
[19].https://www.boundless.com/sociology/textbooks/boundless-sociology-textbook/deviance-social-control-and-crime-7/crime-65/white-collar-crime-390-7850/
[20].http://www.encyclopedia.com/topic/white-collar_crime.aspx
[21].http://cyberlaws.net/cyberindia/articl es.htm
[22] http://www.cyberlawsindia.net/
[23]http://satheeshgnair.blogspot.com/2009/06/selected-case-studies-oncyber- crime.html
[24]http://www.cybercellmumbai.com/