Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.7641969

LAW OF DATA THEFT: A COMPARATIVE ANALYSIS

G .Mallikarjun
Assistant Professor, NALSAR University of Law.

Abstract

Until the dawn of the 20th century, incidents of crime where limited to physical attacks on individuals or the society at large. However with the advent of the computers and the internet, criminal opportunities have increased tremendously. One of the mostly widely committed internet crimes is that of data theft. The earliest incident of data theft was reported in the year 1962, where an insider hacked into the MIT's Compatible Time-Sharing System and stole information.[1] Several incidents of internet data theft have been reported ever since the most famous being the Ellery System's case in 1994. In this case, an employee of the American firm transferred the entire source code of the firm via the internet to a Chinese competitor forcing the firm to file for bankruptcy.[2]

Incidents of data theft aren't limited to western developed countries, they plague developing nations as well, in particular India. The incidents of data theft in India have multiplied at an escalating pace over the past decade. The most recent case, being the ICICI bank case at Pune, where two IIT Kanpur directors were duped of several lakhs of rupees electronically after an internet attack targeted their bank accounts. It is alleged that the victim's confidential information was leaked by an insider that facilitated the theft.[3] With the growing occurrences of data theft in India the question that one needs to ask is whether the laws protecting data in India are adequate or whether they need to be revamped in light of the numerous technological advancements. The author in this paper analyses the criminal behaviour which causes an individual to resort to data theft and demonstrates that a change in the laws governing data protecting would increase deterrence. Several criminological theories suggest that if the punishment is higher and opportunity to commit crime is lower, then the occurrence of data theft would consequentially reduce. Thus the author argues for an amendment to data protection laws which increase the punishment and enforcement mechanisms which would inevitable reduce crime rates. The author has analysed the data protection laws followed in an international setting in light of the nuanced angle of data theft, specific analysis has been carried out with the data protections laws in the United Kingdom as it is one of the few regions in the world to enact strict data protection legislations keeping in sync with to the theories of causation of crime.

Insider Crimes

[1] Robert McMillan, *The World First Computer Password That Too Was Useless?* (last accessed 9th October 2013) http://www.wired.com/wiredenterprise/2012/01/computer-password/?utm_source=UniBul.
[2] Stephen W. Magnan, *We Are Our Worst Enemy* (last accessed 9th October 2013) https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/summer00/art08.html
[3] Abhijit Sathe, *Former IIT Kanpur director conned by cyber criminals* (last accessed 9th October 2013) http://www.mid-day.com/news/2013/sep/160913-pune-former-iit-kanpur-director-conned-by-cyber-criminals.html.

The term "insider" has been defined to refer to "an individual who has private access computer systems otherwise restricted to the public, [4] it includes but is not limited to contractors and consultants, temporary helpers, and even personnel from third-party business etc."[5] Consequentially the term "insider crime" has been defined to refer to "an intentional manipulation or dissemination of private secure data available on organisation's network system by an individual who has access to the organisation's network otherwise restricted to the public".[6] In other words, an "insider crime" is the intentional manipulation or misuse of data by a person authorised to access it.[7]

Insider crimes can be broadly divided into four main categories namely theft, espionage, sabotage and excessive use of the organisational network for personal matters.[8] The last category will not be discussed as it falls outside the ambit of the scope of this project as it is not an illegal act but may be subject to disciplinary actions by the employer.

Theft

The stealing of private data whether in the form of client contacts, trade secrets, confidential transactions or intellectual property by an employee amounts to data theft and is a criminal offence. A case study conducted by Prof. Shaw and his colleagues revealed that the primary justification provided for stealing was that "the accused had contributed to the work that was stolen by him and he had rights or a sense of entitlement over the work that was never given to him by his employers."[9] Some of the factors that were shown to motivate such criminals were ability to start a new business, high financial gains, lack of punishment or low risk of getting caught.[10]

Espionage and Sabotage

While theft and espionage might seem to be the same act for a layman, there does exist a nuanced difference between them. Theft is carried out primarily for personal gains only while espionage on the other hand is the process of employing an individual to work in a competitor's organisation to steal confidential data.[11]

Sabotage refers to "malicious activity in which the insider's primary goal was to sabotage some aspect of an organization or to direct specific harm toward an individual or individual's. [12]. The motive for espionage and sabotage is similar however people who sabotage their company of employment are of two types those who carry out the act for personal benefits or as a result of some personal vendetta against their employees and those who carry out the act under the instructions of a third party.[13] The behaviour of people who commit acts of both espionage

[4] Department of Homeland Security (US) research project "Human Factors, Awareness, and Insider Threats", 2007-2009.
[5] Schultz, E., & Shumway, R. (2001). Incident response: a strategic guide to handling system and network security breaches. Indianapolis: Sams.
[6] US-CERT. (2012). Common Sense Guide to Mitigating Insider Threats, 4th Edition. http://www.sei.cmu.edu/reports/12tr012.pdf.
[7] Sarah Lowman, *Criminology of Computer Crimes*(last accessed 9th October 2013) http://lowmanio.co.uk/share/TheCriminologyofComputerCrime.pdf
[8] *ibid.*
[9] Moore Trzeciak, Cappelli, Caron, Shaw, *Insider Theft of Intellectual Property for Business Advantage: A preliminary* 1st INTERNATIONAL WORKSHOP ON MANAGING INSIDER SECURITY THREATS, 1-22 WEST LAFAYETTE PRUDE UNIVERSITY (2009).
[10] *ibid.*
[11] Stephen R. Band, Dawn M. Cappelli Lynn F. Fischer, Andrew P. Moore, Eric D. Shaw, Randall F. Trzeciak, *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis* AVAILABLE AT CERT, (LAST accessed 9th October, 2013) www.cert.org/archive/pdf/06tr026.pdf.
[12] *ibid*.
[13] Sarah Lowman, *Criminology of Computer Crimes*(last accessed 9th October 2013) http://lowmanio.co.uk/share/TheCriminologyofComputerCrime.pdf

and sabotage are similar. They have the perception that the rewards of committing the crime are higher the consequences of being caught. They also believe the likelihood of getting caught is almost negligent.[14]

The common trait among insiders who commit crime is that they believe that the reward of the crime is high and the likelihood of getting caught is low, additionally even if they do get caught the believe that the sanctions against them don't outweigh the benefits of the reward. This belief ties in with the rational choice theory of why criminals commit crimes, which has been discussed in the next segment.

Data Protection Laws

The primary target of the above mentioned insider crimes are private and confidential data, which can be sold to outsiders at very high prices. There have been several laws enacted across the world to protect data. The European Union however is the only region where countries have enacted specialised legislations to protect data theft. The Council of Europe follows the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 1981. This is an international convention that came into force on 28th January 1981.[15] It mandates for legislation protecting individual as well as governmental data. The United Kingdom and other states of the European Union have an Information Controller or its equivalent data protection authority. All sensitive and private data is to be registered and updated at the office the Information Controller.[16]

Other countries such as the United States, China, and India do not have an organisation whose sole aims is to monitor breaches in private data.[17] While India and USA have laws regulating data theft they're as developed or effective as that of the European Union. China on the other hand has no national legislation to protect their data. Data theft is handled under Chinese tort law, criminal law and various ordinances (China's consumer protection rules).[18]

As seen in the section that the primary aim of all insider crimes is the stealing of confidential information, however in order to bring about a policy change with regard to deterrence, one needs to understand the rationale in a criminal's mind when they resort to such acts.

2: CRIMINOLOGICAL THEORIES

There are two primary theories that are voiced while developing policies which aim at increasing deterrence rates are the *Rational Choice* theory and the *Routine Activity* theory. The former concentrates on the criminal's ability to make sound decisions while that later shifts the focus from the decision making process to the factors influencing the decision making process.

Rational Choice Theory

The Rational Choice theory was developed from the Classical Criminological theory. The classical criminological theory was developed in the late eighteenth century by Cesare Beccaria and Jeremy Bentham.[19] The theory propagated the belief that all criminals are free, rational and

[14] Ariss Naykodym and *Computer Action and Addiction* JOURNAL OF LEADERSHIP ACCOUNTABILITY AND ETHICS (2008)
[15] CHRIS REED AND JOHN ANGEL, COMPUTER LAW (UNIVERSAL PUBLICATIONS 4TH ETD CHAPTER 13, 442) (2002).
[16] BAKER HOSTETLER, INTERNATIONAL COMPENDIUM ON DATA PROTECTION LAWS (Last accessed 9th October 2013) http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf.
[17] *ibid*.
[18] *ibid*.
[19] HUGH D. BARLOW, INTRODUCTION TO CRIMINOLOGY 93 (HARPER COLLINS 5TH ETD 2000).

hedonistic people. Prof. David Garland in relation to classic criminology stated that "criminals by nature (with an exception of the mad and infant) were like all other individuals who possessed the faculties of will, responsibility and reason."[20] Thus criminals were beings who were capable of making reasoned decisions with regard to whether to commit a crime or not. They choose to commit a crime only because they're actions are likely to result in more benefits than losses.[21]

The economic model theory propounded by Gary Becker is a modern variation to the classical criminological theory. The theory is based on two primary assumptions that *first* individuals choose to commit crimes and *second* that all individual's make the similar decisions when put in similar circumstances.[22] Based on these two assumptions theorists state that individuals commit crime if the satisfaction or utility derived from the act of the crime is higher than the act of not committing the crime.[23]

This theory was further developed by Stafford, Warr Patternoster, Cornish and Clarke Matsueda into the Rational Choice theory. The Rational Choice theory which extends the reasoning adopted in the economic model theory states that while individuals deliberate upon the decision of whether to commit crime or not they consider the expected rewards, the risks and alternative actions to reduce risk. It is only after this carefully planned out process do individuals actually engage in criminal behaviour.[24] Furthermore the rational choice model states that criminals follow this detailed process not only while making the decision to commit the crime or not but also while choosing one particular crime over the other or targeting a specific individual over another. An analogy can be drawn between residential robbery and theft committed via the internet. In a study conducted by Prof Thomas Reppetto, he interviewed several offenders arrested for residential burglary. When asked what factors they considered while deciding to commit the robbery, the most commonly cited factors were occupancy of the house, affluently neighbourhood and police patrol in the area.[25] The factors considered are a majorly influenced by the chances of getting caught and the profit that is likely to be obtained after committing the crime.

breach.

Objective of Rational Choice Theory in Data Theft Deterrence Policies:

Thus applying this theory to policies created for data protection, it would be safe to state that any policy that results in the creation of a strong capable guardian would act as deterrence for committing data theft crimes.

Observations:

Thus any data theft policy which aims at increasing rates of deterrence must enhance two specific provisions ***first*** there must be a punishment or actions against the offender so as to outweigh the benefits of the act of committing the crime and ***second*** there should be a strong

[20] DAVID GARLAND, PUNISHMENT AND WELFARE: A HISTORY OF PENAL STRATEGIES 120 (GROWER 1985).
[21] *ibid*.
[22] HUGH D. BARLOW, INTRODUCTION TO CRIMINOLOGY 93 (HARPER COLLINS 5TH ETD 2000).
[23] *ibid.*
[24] THOMAS REPPOTT, RESIDENTIAL CRIME 67 (CAMBRIDGE MASS 1974).
[25] THOMAS REPPOTT, RESIDENTIAL CRIME 67 (CAMBRIDGE MASS 1974).

enforcement mechanism that acts as a capable guardian preventing individuals from engaging in such insider crimes.

3: INTENRATIONAL DATA PROTECTION LAWS

With the advent of globalisation and cross national transactions, there is a substantial percentage of data being transferred between countries. In the absence of a regulatory authority, the scope for manipulation and theft of such data via the internet is very high. Furthermore a growing trend of stealing, data by insiders working in a branch of a multinational company situated in country with minimal legislative protections has been observed.[26] International organisations such as the European Council, United Nations, OECD and the European Union have undertaken programmes to ensure harmonizing data protection legislations across the world.

A. The Council of Europe

The Council has enacted the International Convention for the protection of individuals with regard to Automatic Processing of Personal Data 1981.[27] The convention came into force in October 1985 and now has been ratified by a majority of the countries of the Council. The main aim of the treaty is strengthen cross border transfer of data, while harmonizing the all so as to provide equal punishment regardless of the jurisdiction for insiders committing data theft crimes.[28] Under this part II of this convention, certain core principles are enshrined which provide for free flow of transborder data, while ensuring that each country sets up a regulatory authority that addresses issues of data theft in particular.[29]

B. Organisation for Economic Cooperation and Development

The main motive behind protecting data for the OECD was to improve trade and economic advancement. The OECD setup the Working Party on Information Computers and Communications Policy which created the Group of Government Experts on Transboundary Data Barriers and the Protection of Privacy group.[30] This group was instrumental in drafting the OECD guidelines in 1979 and which were later adopted in 1980. [31] The guidelines are similar to that of the Council of Europe's. The guidelines provide for eight basic principles which are "Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle, Use Limitation Principle, Security Safeguard Principle, Openness Principle, Individual Participation Principle and Accountability Principle".[32] The two important principles which govern data protection are the *Security Safeguard Principle,* which states that reasonable measures should be taken to ensure no authorised access is allowed and

[26] CHRIS REED AND JOHN ANGEL, COMPUTER LAW 445 (UNIVERSAL PUBLICATIONS 4TH ETD 2002)
[27] Convention for the protection of individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28th January 1981.
[28] CHRIS REED AND JOHN ANGEL, COMPUTER LAW 446 (UNIVERSAL PUBLICATIONS 4TH ETD 2002).
[29] Explanatory Report, Convention for the protection of individuals with regard to Automatic Processing of Personal Data 1981 (last accessed October 9 2013) http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm
[30] *ibid*.
[31] Organisation for Economic Cooperation and Development, *Guidelines on the Protection of the Privacy and Transborder Flows of Personal Data,* 1980.
[32] *Ibid* (last Accessed 9th October 2013)
http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part2

Accountability Principle, which states that the data controller is held responsible for all failures to regulate data protection.[33]

United Nations

The guidelines framed by the United Nations covers two sectors *one* the law providing for minimum guarantees of data protection for individuals. These laws larger mirror both the Council of Europe and the OECD's guidelines, with an exception of the supervision and sanction clause that "provides that date protection authorities shall offer guarantees of impartiality, independence *vis a vis* a person or agencies responsible for protection" and the *second* sector governs laws applicable to governmental data.[34]

European Union

Data protection laws have been given a lot of importance in the European Union. Over 25 countries[35] have their revised and amended their own legislation. While other countries outside the European Union such as the United States, Japan and Australia have also adopted data protection laws, they're laws are evasive and provide less protection to users.

The Legal Affairs Committee has been the primary organisation that has worked to develop data protection in the European Parliament. The committee brought into effect the "directive" which concerns the regulatory framework for data protection.[36] However till date only 5 countries have adopted the "Directive" into their national legislation.

The above international mechanism primary aim at free flow of data throughout the country, with regard to national legislative measure which are stringent and effectively protect data within the country, the best example would be the data protection legislations followed by the United Kingdom.

4: UNITED KINGDOM'S DATA PROTECTION LAWS

In the United Kingdom, there are two primary legislations that aim at protecting data; The Data Protection Act 1998 and the Computer Misuse Act 1990.

A. Data Protection Act 1998

The Data Protection Act includes personal data within its ambit. Personal data is defined "to consist of data that relates to a living individual who can be identified from the data, or from that and other data or information in possession of the data user."[37] The Data Protection Act provides for a Data Protection Commissioner. The Commissioner has the duties to promote data protection norms and observance.[38] In addition, Commissioners are given unique powers of issuing notices in order to obtain information,[39] apply to the court for a warrant and institute suits for search and seizure procedures,[40] issue notices for non compliance [41] and instigate prosecution under the Act.

[33] *ibid*
[34] *ibid.*
[35] Austria, Belgium, Checz and Slovak Republic, Denmark, Finland, France, Germany, Greece, Guernsey, Hungary, Iceland, Ireland, Isle of Man, Italy Jersey, Luxembourg, Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland and the United Kingdom.
[36] Directive 95/ 46 / EC Protection of Individuals with regard to the processing of personal data and the free movement of such data.
[37] Section 1, The Data Protection Act 1998.
[38] Section 51, of the Data Protection Act 1998.
[39] Section 43 of the Data Protection Act 1998
[40] Section 9 of the Data Protection Act 1998
[41] Section 40 of the Data Protection Act 1998.

An individual who is under the impression that his personal data has been compromised can directly approach the Commissioner and request the Commissioner to carry out an inquiry.[42] Pursuant to the Act, the victim has the right to be compensated for situations of inaccuracy, loss destruction of data or authorised access.[43] Furthermore, the said Act permits to piercing of the corporate veil to hold directors of the company liable for acts which resulted in unauthorised usage.[44]

B. Computer Misuse Act 1990

The Computer Misuse Act punishes data theft i.e. unauthorised use of the computer or network system. Section 3 of the said Act states that three essentials that need to be proved before a person can be held guilty of an offence are *one,* there should be an act of unauthorised access, *two* the person should have had the intent to secure unauthorised access and *three,* the person must have had the requisite knowledge at the time of committing the crime that the access to the data was unauthorised.[45] A person who is held guilty of the offence is liable to be sentenced to five years imprisonment.[46] An innovate change has been brought about in Singaporean law, where the accused is made liable to compensate the victim for the damage caused, by the unauthorised access

C. ICO Guidelines

The International Commissioner's Office, is an independent body setup in the United Kingdom to uphold data protection norms for individuals. The ICO lays down guidelines to in order to assist individuals and companies to better protect they're data. The guidelines also provide for security training to the staff.

5: INDIA

A. Indian Penal Code

The Indian Penal Code 1860[47] punishes crimes of theft. The theft is defined under Section 378 of the IPC as "an act of dishonestly taking any moveable property out of the possession of any person without that person's consent."[48] The term movable property is defined under Section 22 of the IPC and it refers to only corporeal property of all kinds with an exception of land and everything else attached to the earth.[49] Thus data which is stolen and stored in floppies hard disks or CDs are covered under the provisions of the IPC. However if the stolen is data is transmitted via the internet the crime is not punishable under the IPC as data is intangible in nature.

There have been lawmakers[50] that have argued that crimes of data should be punished under Section 405 of the IPC which deals with criminal breach of trust. The Section states that "*however, being in any manner entrusted with* ***property,*** *or with any* ***dominion over property****, dishonestly misappropriates or converts to his own use that property, or dishonestly uses or*

[42] Section 42 of the Data Protection Act 1998
[43] Section 22 and Section 23 of the Data Protection Act 1998.
[44] Section 61 of the Data Protection Act 1998
[45] Section 3 of the Computer Misuse Act 1990.
[46] Section 3(7) of the Computer Misuse Act 1990.
[47] Hereinafter IPC.
[48] Section 378 of the IPC.
[49] Section 22 of the IPC.
[50] Kaviraj Singh, *Data Theft and Security Law In India* (last accessed 9th October 2013) http://www.delhilaw.firm.in/articlenews/data_theft_security.htm;

disposes of that property in violation of any direction of law prescribing the mode in which such trust is to be discharged, or of any legal contract, express or implied, which he has made touching the discharge of such trust, or wilfully suffers any other person so to do, commits 'criminal breach of trust".[51] The section uses the term property and not movable property hence data theft can be covered within its ambit. Section 406 of the IPC punishes acts of criminal breach of trust with imprisonment up to 3 years or fine or both.[52] In the absence of any specific provision to protect data theft under the country's primary penal statute one needs to look at specific legislations.

B. Information Technology Act 2000

In India data theft crimes are prosecuted chiefly under Section 43 of the Information Technology Act 2000.[53] Section 43 of the IT Act prosecutes illegal or unauthorised access,[54] unlawful downloading or copying of data[55] and unauthorised modifying, destroying, recording and transmitting of data or programmes stored in computers, computers systems and computer networks.[56] The punishments for crimes of data theft have been provided for under Section 66 of the IT Act. The act punishes the offender with up to 3 years imprisonment or up to rupees 5 lakhs or both.[57] Furthermore the Act makes it obligatory for a body corporate possessing or handling data personal data to protect an individual personal data failure to do so results in liability to pay damages in terms of compensation to the affected person.[58]

Lawmakers have argued that crimes of data theft should be punishable under Section 72 of the IT Act, as it amounts to a breach of privacy and confidentiality also. The punishment prescribed is imprisonment up to two years and fine up to one lakh.[59] However till date the there have been no cases of data theft prosecuted under Section 72 of the IT Act.

Regardless of the whether the provisions of the IT Act apply or whether the provisions of the IPC are invoked the imprisonment is 3 years or less and the fine imposed is 5 lakhs or less. Data theft crimes are result in providing the criminal with profits margins that run into cores. Punishment of meagre 5 lakhs doesn't act as an adequate deterrence. For these reasons and more the research has suggested some of the following changes in the system.

CONCLUSION

The following suggestions I make are with regard to developing a system in India, in which deterrence of data theft is given priority over punishment after committing of the crime.

A. International Front

The international policies followed by the European Union and the Council of Europe, have been embodied by both the United Nations and OECD. These policies all aim at uniform treatment. Though India is a member to the UN and works closely with the OECD, it has made no effort to change its data protection laws so as to bring uniformity. The suggestion, which I make, is precisely this, revamping of the system so as to achieve international uniformity.

[51] Section 405 of the IPC
[52] Section 406 IPC.
[53] Hereinafter IT Act.
[54] Section 43 (a) Information Technology Act 1998.
[55] Section 43(b), Information Technology Act 1998.
[56] Explanation 2 (i) (a) Information Technology Act 1998.
[57] Section 66 of the Information Technology Act 1998.
[58] Section 43 A of the Information Technology Act 1988.
[59] Section 72 of the IT Act.

B. National Front

On the domestic front, the legislation should be amended in tune with the *Rational Choice Theory* and *Routine Activity Theory* so as to promote deterrence.

The Rational Choice Theory indicates that a higher penalty would deter a person from committing the crime. Thus, the suggestion I make is that, instead of imposing a merger punishment of Rs 5 lakhs or less in cases which result in crores of profits for the offender, India should follow the Singaporean system of punishment for crimes of data theft. They hold the accused liable to compensate the victim for all the damages caused by such unauthorised access. Thus there is no cap on the fine, but it runs in concurrence with the profits obtained from such unauthorised access.

The next suggestion I make is in accordance with the Routine Activity Theory, which indicates that incidents of deterrence would be increased if there was a supervisory mechanism. While India does have a supervisory mechanism in place in the form of Anti-Cyber Cells, the functioning of these units is hindered by several factors. The most important being the judicial backlogs, individuals who are arrested through these Anti-Cyber Cells investigations are let out on bail and aren't prosecuted for several years.[60] Thus I propose that there should be a fast track court to try these cases so as to strengthen the efforts and functioning of these Cells. A regime that takes into account the above made observations and implements the suggestions proposed will definitely be a regime in which will see a drastic drop in data theft rates.

BIBLIOGRAPHY

A. Articles And Journals

- Ariss Naykody, *Computer Action and Addiction* JOURNAL OF LEADERSHIP ACCOUNTABILITY AND ETHICS (2008)
- BAKER HOSTETLER, INTERNATIONAL COMPENDIUM ON DATA PROTECTION LAWS (Last accessed 9th October 2013) http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/International-Compendium-of-Data-Privacy-Laws.pdf
- CHRIS REED AND JOHN ANGEL, COMPUTER LAW (UNIVERSAL PUBLICATIONS 4TH ETD CHAPTER 13, 442) (2002).
- CHRIS REED AND JOHN ANGEL, COMPUTER LAW 445 (UNIVERSAL PUBLICATIONS 4TH ETD 2002)
- DAVID GARLAND, PUNISHMENT AND WELFARE: A HISTORY OF PENAL STRATEGIES 120 (GROWER 1985).
- HUGH D. BARLOW, INTRODUCTION TO CRIMINOLOGY 93 (HARPER COLLINS 5TH ETD 2000).
- Kaviraj Singh, *Data Theft and Security Law In India* (last accessed 9th October 2013) http://www.delhilaw.firm.in/articlenews/data_theft_security.htm;
- Lawrence Cohen and Marcus Felson, *Social Change and Crime Rate Trends A Routine Approach Activity* AMERICAN SOCIOLOGICAL REVIEW 90- 118 (1980)

[60] Alistair Maughan, Miriam Wugmeister, Diljeet Titus, *Outsourcing to India: Dealing With Data Theft and Misuse* http://www.computerworld.com/s/article/9004707/Outsourcing_to_India_Dealing_With_Data_Theft_and_Misuse?taxonomyId=14&pageNumber=3

- LAWRENCE COHEN, AGAINST CRIMINOLOGY 44 (BRUNSWICK 2ND ETD 1988)
- Lawrence Cohen, David Cantor, James Klugel, *Robbery victimisation in the US: Analysis of non random event* SOCIAL SCIENCE QUARTERLY 62 (1981)
- Moore Trzeciak, Cappelli, Caron, Shaw, *Insider Theft of Intellectual Property for Business Advantage: A preliminary* 1st INTERNATIONAL WORKSHOP ON MANAGING INSIDER SECURITY THREATS, 1-22 WEST LAFAYETTE PRUDE UNIVERSITY (2009).
- Randall F. Trzeciak, *Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis* AVAILABLE AT CERT, (LAST accessed 9th October, 2013) www.cert.org/archive/pdf/06tr026.pdf.
- Sarah Lowman, *Criminology of Computer Crimes*(last accessed 9th October 2013) http://lowmanio.co.uk/share/TheCriminologyofComputerCrime.pdf
- Sarah Lowman, *Criminology of Computer Crimes*(last accessed 9th October 2013) http://lowmanio.co.uk/share/TheCriminologyofComputerCrime.pdf
- Schultz, E., & Shumway, R. (2001). Incident response: a strategic guide to handling system and network security breaches. Indianapolis: Sams.
- Stephen R. Band, Dawn M. Cappelli Lynn F. Fischer, Andrew P. Moore, Eric D. Shaw,
- THOMAS REPPOTT, RESIDENTIAL CRIME 67 (CAMBRIDGE MASS 1974).

B. Treaties and Reports

- Convention for the protection of individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28th January 1981.
- Directive 95/ 46 / EC Protection of Individuals with regard to the processing of personal data and the free movement of such data.
- Explanatory Report, Convention for the protection of individuals with regard to Automatic Processing of Personal Data 1981 (last accessed October 9 2013) http://conventions.coe.int/Treaty/EN/Reports/HTML/108.htm
http://www.sei.cmu.edu/reports/12tr012.pdf
- Information Technology Act 1998.
- Organisation for Economic Cooperation and Development, *Guidelines on the Protection of the Privacy and Transborder Flows of Personal Data,* 1980.
- The Computer Misuse Act 1990.
- The Data Protection Act 1998.
- US-CERT. (2012). Common Sense Guide to Mitigating Insider Threats, 4th Edition.