TECHNOLOGY CRISIS AND CYBER CRIMES: INDIAN PERSPECTIVE

Dissertation submitted to National Law University and Judicial Academy, Assam
in partial fulfilment for award of the degree of

MASTER OF LAWS/

ONE LL. M DEGREE PROGRAMME

Supervised by:
Name: Mr. Thangzakhup Tombing
Designation: Assistant Professor of Law

Submitted by:
Name: Hardik Vyas
ID: SM0219008
LL. M (2019-2020)

National Law University and Judicial Academy, Assam
August, 2020

SUPERVISOR CERTIFICATE

It is to certify that Mr. **HARDIK VYAS** is pursuing Master of Laws (LL. M.) from National Law University and Judicial Academy, Assam and has completed his dissertation titled "**TECHNOLOGY CRISIS AND CYBER CRIMES: INDIAN PERSPECTIVE**" under my supervision for fulfilment of the award of degree for **MASTER OF LAWS/ ONE YEAR LL.M DEGREE PROGRAMME**. The research work is found to be original and suitable for submission.

Date: 17/08/2020

T. Tombing

____

NAME OF THE SUPERVISOR: Mr. Thangzakhup Tombing

DESIGNATION: Assistant Professor of Law.
National Law University and Judicial Academy,
Assam.

DECLARATION

I, **HARDIK VYAS**, is pursuing Master of Laws (LL. M.) from National Law University and Judicial Academy, Assam, do hereby declare that the dissertation titled "**TECHNOLOGY CRISIS AND CYBER CRIMES: INDIAN PERSPECTIVE**" is an original work and has not been submitted, either in part or full anywhere else for any purpose, academic or otherwise, to the best of my knowledge.

Date: 17/08/2020

Hardik

NAME OF THE CANDIDATE: Hardik Vyas

COURSE: LL.M (2019-2020)
National Law University and Judicial Academy,
Assam.

ACKNOWLEDGEMENT

“A reputation once broken may possibly be repaired, but the world will always keep their eyes on the spot where the crack was.”

- Joseph Hall

At the outset, it has been a mammoth effort and possible only because I have been provided the opportunity and creative freedom to do as I wanted. For this, I would like to express the deepest gratitude towards Mr. Thangzakhup Tombing, Assistant Professor of Law, who has the attitude and substance of brilliance; he incessantly and cogently conveyed a spirit of adventure in regard to research and an excitement in regard to teaching. Without his guidance and persistent help this dissertation would not have been possible.

I would also like to express my special gratitude towards Dr. Topi Basar, Associate Professor of Law and Coordinator for LL.M batch 2019-20 for her valuable guidance with regards to Intellectual Property Rights and Cyber Laws. I would like to specially thank Dr. J. S. Patil, The Honorable Vice-Chancellor of National Law University and Judicial Academy, Assam for sharing his vast knowledge in the field of legal research and methodology through his vigorous lectures.

I would also like to thank the Librarian and the whole staff of NLUA Library, IT Section for their immense help and cooperation in making all the relevant material available in this hard times of pandemic (COVID-19) in India.

I would like to thank NLU Assam as an institute where I not only completed my degree but also grew as an individual at the same time.

Finally, I gratefully acknowledge the help, support and advice of all the authors whose writing is utilized in my studies and academic non-academic staff, my parents and fellow batch-mates for their unending support and providing me all the necessities required at different stages for the preparation of this empirical study.

Hardik Vyas
SM0219008
LL. M (2019-2020)

PREFACE

Technology is the set of skills, methods and processes used mainly to achieve the targeted objectives. It is that branch of knowledge which deals with the innovation and determining factor of technical means and their interrelation with life, society and the near environment. Crisis is the situation of instability or danger towards the social, economic, political or international affairs. Technology Crisis is disruption in the application of any set of technology arises mainly out of human errors or natural disasters. It mainly occurs due to complexity of technology or due to unpreparedness towards the application of such technology or inadequate measures taken due to non-readiness towards the use of such technology. Moreover, Cybercrime is the recent and perhaps one of the most critical problem which needs to be considered through various facets in the recent times. If conventional crime regarded as genus, then cybercrime would be its species where the computer or any other similar object to be used as a subject in order to conduct or constitute any crime.

In present times, it is important for technology-enabled industries and organizations in India to prepare themselves, mainly such corporations dealing with regular high-level technology, to equip themselves in order to apply various curative measures which make them prepared beforehand in managing such technological crisis for the present and future conditions. India is already facing high threat of cybercrimes which needs to be properly addressed along with their strong preventive measures and stringent legal framework in order to curb this menace in efficient manner. This paper will thereby focus on the status of implementation of the present laws in India in order to know whether such laws are sufficing to ensure the protection of such organizations and prepare them for needful prevention from such problems.

Hardik Vyas
SM0219008
LL. M (2019-2020)

TABLE OF CASES

TABLE OF STATUTES

- **INDIAN STATUTES:**
- 1860, Indian Penal Code.
- 1872, Indian Evidence Act.
- 1885, The Telegraph Act.
- 1950, Constitution of India.
- 1957, Copyright Act.
- 1973, Criminal Procedure Code.
- 1999, Trademark Act.
- 2000, Information Technology Act.
- 2008, The Information Technology (Amendment) Act.

- **INTERNATIONAL STATUTES:**
- **United Kingdom:**
- 1990, Computer Misuse Act.
- 1998, Data Protection Act.
- 2006, Computer Police & Justice Act.

- **United States of America:**
- 1872, California's Penal Code.
- 1970, United States Federal Criminal Code.
- 1986, The Computer Fraud and Abuse Act.
- 2001, US Patriot Act.

- **Canada:**
- 1985, Criminal Code of Canada.
- 2003, Council of Europe Convention on Cyber Crime, Canada.

- **Australia:**

- 2001, Cyber Crime Act.
- 1995, The Criminal Code Act.

- **Germany:**
- 1990, Federation Data Protection Act.
- 1997, Telecommunications Act.
- 2002, Federal Data Protection Act.

- **France:**
- 1958, France Council of European Directives.
- 1992, French Intellectual Property Code.

- **Spain:**
- 1870, Spanish Penal Code.

- **Philippines:**
- 2000, Philippines E-commerce Act.

- **Sri Lanka:**
- 2007, Computer Crime Act.

- **Bangladesh:**
- 2004, Bangladesh Cyber Crime Act.

- **Pakistan:**
- 2007, Pakistan Cyber Crime (Prevention of Electronic Crimes) Bill.
- 2016, Cyber Crime (Prevention of Electronic Crimes) Act.

❖ INTERNATIONAL BODIES AND CONVENTIONS:

- 1883, The Paris Convention.
- 1886, The Berne Convention.
- 1947, General Agreement on Tariff and Trade (GATT).
- 1966, The United States Commission on International Trade Law (UNCITRAL).
- 1970, The World Intellectual Property Organisation (WIPO).
- 1995, The World Trade Organisation (WTO).
- 1995, Trade Related aspect of Intellectual Property Rights (TRIPS).
- 1996, WIPO Copyright Treaty.
- 1998, Internet Corporation for Assigned Names and Numbers (ICANN).

TABLE OF ABBREVIATIONS

S. No.	Abbreviation	Full form
01	¶	Para
02	¶¶	Paras
03	Art.	Article
04	&	And
05	AIR	All India Reporter
06	ANSI	American National Standards Institute
07	ANSNET	Advanced Network Service Net
08	APIs	Application Programming Interfaces
09	ATM	Automatic Teller Machine
10	BC	Banking Cases
11	BEA	Base Erosion Approach
12	BPO	Business Process Outsourcing
13	BSD	Berkeley Software Distribution
14	CA	Certifying Authority
15	CCA	Controller of Certifying Authorities
16	CCTLD	Country Code Top Level Domain
17	CD	Compact Disc
18	CRAC	Cyber Regulations Advisory Committee
19	Corp.	Corporation
20	Cr. L. J	Criminal Law Journal
21	Cr.P.C	Criminal Procedure Code
22	CSS	Content Scamble System
23	CTLR	Computer and Telecommunication Law Review
24	DLT	Delhi Law Times
25	DNS	Domain Name System
26	DSC	Digital Signature Certificate
27	DVD	Digital Versatile Disc

28	EC	European Commission
29	E-Com	E-Commerce
30	Econ.	Economic
31	Ed.	Edition
32	EDI	Electronic Data Interchange
33	EPO	European Patent Office
34	EPC	European Patent Convention, 1973
35	FS	Free Software
36	GATT	General Agreement on Tariff and Trade
37	GIF	Graphic Interchange Format
38	GIIC	Global Information Infrastructure Commission
39	GPL	General Public License
40	GTLD	Generic Top Level Domain
41	HREF	Hypertext Reference
42	HTML	Hyper Text Markup Language
43	HTTP	Hyper Text Transfer Protocol
44	ICANN	Internet Cooperation for Assigned Names and Numbers
45	ICR	Information and Communication Revolution
46	ILR	Indian Law Reports
47	Inc.	Incorporation
48	IP	Internet Protocol
49	IPC	Indian Penal Code
50	IPR	Intellectual Property Rights
51	IPAB	Intellectual Property Appellate Board
52	ISOC	Internet Society
53	ISP	Internet Service Provider
54	IT Act	Information Technology Act, 2000
55	JILI	Journal of Indian Law Institute
56	J.L.	Journal of Law

57	L.	Law
58	LAN	Local Area Network
59	L. ed.	Lawyer’s Edition
60	LDC	Least Developed Countries
61	LGPL	Lesser General Public License
62	MILNET	Military Net
63	NIC	National Informatics Centre
64	NSP	Network Service Provider
65	OS	Operating System
66	OSS	Operating Source Software
67	p.	Page No.
68	P2P	Peer to Peer
69	PDA	Personal Data Assistance
70	PIL	Public Interest Litigation
71	PLC	Public Limited Company
72	QoS	Quality of Service
73	R & D	Research & Development
74	RAC	Regional Access Coding
75	RAM	Random Access Memory
76	RBI	Reserve Bank of India
77	ROM	Read Only Memory
78	SCC	Supreme Court Cases
79	TLD	Top Level Domain
80	TLT	Trade Mark Law Treaty, 1994
81	TRIPS	Trade Related Aspect of Intellectual Property Rights
82	UBE	Unsolicited Bulk E-mail
83	UDHR	Universal Declaration of Human Rights
84	UK	United Kingdom
85	UN	United Nations

86	URL	Uniform Resource Locator
87	UNESCO	United Nations Education Scientific and Cultural Organization
88	U.S.A	United States of America
89	USPTO	United States Patent and Trademark Office
90	Vol.	Volume
91	V.	Versus
92	WAN	Wide Area Network
93	WIPO	World Intellectual Property Organization
94	WCT	WIPO Copyright Treaty
95	WIPO	World Intellectual Property Office
96	WTO	World Trade Organization
97	WWW	World Wide Web

GLOSSARY OF COMPUTER RELATED TECHNICAL TERMS (ACRONYMS):

1. **Archie:** It is a file retrieval tool that allows a user to download files from a Server on to his/her computer.
2. **Bio-metrics:** A set of Science based techniques that deal with individual's biological characteristics such as fingerprints, retinal pattern, voice print, palm print etc. for the purpose of ensuring authentication.
3. **Blogs:** It is a website where entries are commonly displayed in a chronologically reverse order.
4. **B.O.:** Bank Office.
5. **Boot Disk:** It contains Special hidden start-up files and others program to run a computer.
6. **Boot Sector Infectors:** These are most common types of viruses which are easy to make and spread quickly and effectively.
7. **Browser:** It is a software application used to locate and display web-pages e.g. Microsoft Internet Explorer or Netscape Navigator.
8. **Bug:** A programming error in a software program which can have unwanted side-effects e.g. Y2K problem.
9. **Cache:** A temporary memory area set aside to store information which is most frequently accessed in a computer. It is used to enable a computer to operate at a high speed.
10. **Caller ID:** A service which sends the telephone number of the caller to the called party.
11. **Ciphers:** A cipher is a method of encrypting text (concealing its readability and meaning).
12. **Cookie:** A program used to measure user's behavior and habits on the internet. Cookies are stored on the user's hard disc for the purpose of identifying him. It is a message given to a web-browser by a web-server.
13. **Crackers**: A person who gains unauthorized access to a computer usually with the intention of manipulating or damaging data.
14. **CRC:** Cyclic Redundancy Check (CRC) is a verification process for detecting transmission errors.

15. **Cryptography:** It is a process of converting a message into an equivalent version that is not understandable by the unauthorized users. The converse process of making it understandable is called as decryption.
16. **Database:** It is a data structure used to store organized information.
17. **Data Diddling:** It is a kind of attack which involves altering the raw data just before a computer processes it and then changing it back after the processing by computer. It is a cybercrime of common occurrence.
18. **DDoS:** Distributed Denial of Service.
19. **Digital Evidence:** Information having probative value stored or transmitted in the digital form.
20. **DNS Spoofing:** It means the use of Domain Name Server (DNS) with a fictitious cover to gain access to a computer.
21. **Domain Name:** It is the name that identifies a computer or computers on the internet. These names appear as a component of a website's URL.
22. **DoS:** Denial of Service.
23. **Dropper:** It is a virus carrier which drops a virus. It creates a virus file or program on the computer.
24. **E-com:** Electronic Commerce.
25. **E-mail:** It is a fast and efficient way of communication allowing the user to send, receive, forward, answer or delete electronic messages.
26. **Encryption:** It means conversion of data into a secret code.
27. **Font:** It is a certain form of face of a certain style or size.
28. **Firewall:** Hardware and software placed in a Local Area Network LAN) through which all incoming data pass for verification and authentication. It is used to protect certain classified areas of network.
29. **Hacker:** A person who with sufficient knowledge of computer networking and communication gains entry into closed or protected computer systems by outwitting security measures. If the hacker commits any malicious damage, he is called a cracker.
30. **Address:** It is an identifier for a computer or a device on IP network.

31. **LAN:** Local Area Network (LAN) covers limited geographical area such as building, company, university etc. and is usually owned by the user's organization or enterprise.
32. **Logic Bomb:** It is a computer virus which results in data damage or unauthorized data manipulation.
33. **Log in:** It is a combination of information that authenticates user's identity that could be a name and password or ID number and security code.
34. **Modem:** Modulator/Demodulator.
35. **MS Word:** Microsoft Word.
36. **Phishing:** It is an e-mail fraud in which perpetrator sends out a legitimate looking e-mail in an attempt to gather personal information from the recipient. The message appears to be coming from a well-known and trustworthy website.
37. **Phreaking:** The act of gaining unauthorized access to a telephone system or network.
38. **RAM:** Random Access Memory is a space in a computer wherein the operating system programs and data in current use are kept so that they can quickly be reached by computer's processor.
39. **RAT:** Remote Administration Trojan.
40. **ROM:** Read Only Memory is a computer memory on which data has been pre-recorded on ROM chip; it cannot be removed and can only be read.
41. **Salami Attack:** It means series of minor data security attacks that together result in a large attack on computer system.
42. **Spam:** It means to place some message all over and even to a place where it does not belong, in order to attract the attention of such services.
43. **Spamming:** A variety of e-mail bombing consisting of junk mail being downloaded in large quantity.
44. **Stalking:** Any unwanted contract between two persons that directly or indirectly communicate a threat or place the victim in fear.
45. **Trojan Horse:** A hidden program in a computer system meant to modify, damage or destroy the contents of the computer system. It is often used by the hackers to leave a backdoor in the system's protection.

46. **UNIX:** It is a general purpose operating system that has led to many variations targeted at specific market segments.
47. **URL:** Uniform Resource Locator (URL) is a global address of documents and other resources on the world wide website. It is unique address for a file that is accessible on the internet.
48. **Virus hoax:** It is a false warning about computer virus which causes damage to the system.
49. **Web jacking:** It occurs when certain unscrupulous internet hosts turn your browser against you.
50. **Worm:** Once installed, it corrupts certain program files to multiply. It is a self-replicating virus that does not only alter files, but resides in active memory and duplicates itself.
51. **Yahoo:** It is one of the Internet's leading search engines providing links to thousands of other websites.
52. **Zip files:** A compressed file having extension.

TABLE OF CONTENT

"Writing is easy....... all you have to do is to think,

till the drop of blood appear on your forehead"

- Balzac.

ABSTRACT

Over the past decades, World is moving towards the internet for almost everything, be it any information or delivery of any product or any other essential services and the prevalent condition of India is not any different. But, at the same time, in order to maintain efficiency in terms of organizational readiness, it is important to manage prevalent crisis, especially, to focus on the aspect of technological crisis, such as hardware system failure, software failure or any other mechanical damages, it is crucial to manage such crisis which proves as an elementary step towards the cyber friendly space and helps corporates to prepare in advance towards such problems as various professional/technical sectors of India is already facing some high level challenges, such as, there are people who use high-level technologies for the purpose of wrongful activities prohibited by law, most common among them are online theft, hacking, spreading hate messages, creating viruses etc., and moreover many people are still unaware about such problems or even when some people come to know any such incident, the lack of knowledge regarding appropriate remedy leads them towards ignorance of that particular incident, even if such crime has been committed at very basic level and it ultimately motivates such offender to continue such activities and it results in the motivation of various crimes in the cyber space and creates inferiority problems among certain segment of the population which contains both educated and uneducated people and ultimately, due to many such incidents in India, it leads country towards problem of the technology crisis.

To incorporate sound technological balance in the country or to reduce the fear towards data infringement and misappropriation of creation problems, India requires much updated and stronger laws for confronting at equal level with such problems, irrespective of its size or scale. In order to incorporate such provisions or specific laws, it is very crucial to review, revaluate and reassess the current cyber laws of India.

Keywords: Information Technology, cybercrimes, cyber space, infringement, cyber laws

CHAPTER 1

INTRODUCTION

"Any sufficiently advanced technology is indistinguishable from magic"

- **Arthur C. Clarke**

Computer technology is developing in leaps and every coming day the space between the computer technology and computer security technology is growing significantly, thereby it gets a lot of scope for the committing various computer crimes. The ongoing issue is compounded by the fact that most of the computer users are themselves really not really aware about what a computer crime actually means and the quantum of its damage, and many crooks are already exploiting this weakness for their own greed. While those responsible for the prevention of these crimes are somewhere always groping in the dark, the system breakers are busy jumping in and out of so called protected networks, learning about latest security glitches as well as easily discovering bugs and vulnerabilities. These deadly creatures can strike on their aims fatally with impunity and can hide their tracks without leaving a single trace. With more businesses across the world being linked together through the Internet, the use of credit cards being normal, so the problem of cyber security is becoming of greater significance. The Internet has only benefitted criminals by minimizing the cost of attack. While any crime would require physical presence earlier, the Internet has enabled the criminals to target maximum number of people at minimal cost and at the click of button away. People with technology intellect have been grossly misusing this aspect of Internet to generate illegal act in cyberspace. The field of cybercrime is emerging at great pace and new forms of conventional criminal activities in cyberspace are coming to the forefront with the passing of each day. Cybercrimes ranges from the catastrophic to the stage of annoying. Cybercrime is the epidemic confronting our country in this millennium. A cyber-criminal can destroy websites and portals through hacking and viruses, can carry any on-line frauds by transferring funds from one corner to another, gain access to highly classified and sensitive information, lead harassment, bye mail threats or obscene material, conduct tax frauds, can indulge in pornography involving children, and commit several other crimes on the Internet. Which finally lead us to the situation that none is secure in the cyber world.

1.1. RESEARCH BACKGROUND:

This study is mainly based on two facets, firstly, to evaluate the position of Technological Crisis faced by the organizations in India and secondly, to analyze and understand the detailed position of cybercrimes and cyber laws in India. The term ‘Crisis’ can be perceived differently by different people or groups. It is considered by many as an adverse event with the unintended results which proves as threat to the person or organization. Crisis is something which comes suddenly and unexpected in nature. Technological crisis arises mainly due to failure in any technology or its application. Breakdown of machine, corrupted software and system failures give rise to technological crisis. It is emerging as one of the big challenge which turned out as evaluating process of the credibility and reputation of organizations and the perception of their responses during such crises situations. It is pertinent to have coordinated communication and swift dissemination of working knowledge of introduced new technology throughout the hierarchy of organization to contribute towards the crisis communication process. Cybercrimes are technology intensive crimes. They revolve around the technologies and its applications. Cybercrimes are the crimes committed which are mainly based on the human behavior on cyberspace.

There are mainly two technological schools of law: first one is Technology Neutral School and the another is Technology Specific School. The controversy between them was based on the adoption of law. Technology Specific School argues that the law should recognize only one given set of technology or technology standard. That is, law treats other standards as illegal, non- binding and thus not permissible. The main advantage of this School is that it creates a single technology platform for the entire community. The main drawback of this Specific School is that it kills technological innovations and helps to the monopolistic businesses, which is bad practice for the society.

Whereas, Technology Neutral School enumerates about the law which should remain neutral when it comes to giving due recognition to any technology or technology standards. It recognizes all the technologies or technology standards at equal level and does not discriminate between the various technologies. The benefit of this School is that helps in providing efficient and useful technologies for the community. Again, the drawback of this School is that it provides multiple technology platforms and which may lead to increase cost of assimilation of technology for the entire community.

It is pertinent to note that both the technology specific law and the technology neutral law may co-exist side by side at any given point of time. Commonly, it is observed that the developed countries with a wider technology users' base have multiplicity of technology platforms, whereas the developing countries with a narrow technology users' base generally possess common technology platform which may support them to begin with.

The main reason behind that was, in a developing country, technology is at a premium and hence the users are less, whereas, the condition in a developed country is that they have large numbers of users and almost attained maturity stage of technology and hence are multiplicity of technology platforms.

At this juncture, it is really essential to critically analyze the crisis and crisis management, especially, technological crisis through the viewpoint of various organizations and stakeholders in India in order to evaluate how well the organizations are prepared in dealing with such crisis when it occurs through comparative analysis. Recently, various important events in terms of social, economic, political, geographical and towards mankind shows that societies are undergoing from various technological breakdowns/hazards which clearly indicates that the level of technology that could be useful can also turn out to be dangerous for the organizations. Also, to analyze the nature of cybercrimes faced by such technology enabled organizations in India and Judicial steps taken by Indian courts till date, in order to identify the current position and suggestive measures, if any, required to strengthen the current position of cyber laws in India with the perspective of organization or Industries which may help them to enhance their present technological conditions by preparing them for any critical and unforeseeable future contingencies.

1.2. STATEMENT OF PROBLEM:

The problem of this paper deals with the vulnerability of Indian organizations which leads to triggering events regarded as Crisis. Technology based organizations are generally observed having high growth rate and possess ability to create more jobs but at the same time faces tension towards crisis. One such crisis which may hit such organizations are Technological crisis. Technological crises maybe broadly defined as a set of circumstances, which if poorly managed and ignored for a longer span of time may result in bringing an organisation to its knees. The numbers of occurrence of Technological Crises across industries have considerably increased over the years and can no longer be considered as a rare occurrence. Observing the prominence of the situation, it becomes crucial for a manager to be responsive as the environment becomes dysfunctional or during any change required in the inherent processes of the organization. Crises often bring the mangers to the front end of reality, with a set of circumstances they may have not encountered before. Therefore, it is essential that managers should be on their toes or the organisation could be vulnerable towards reoccurrence of such crisis. Further, it can be concluded through these incidents that unless crisis is controlled and managed strategically, growth in the industry and sustainability will not be attained.

In the second phase, this paper also deals with the problems of Cybercrimes in India and critically analyses the prevalent cyber laws in India and discusses about this menace by providing various instances relating to cybercrimes. It also deals with the concept of jurisdiction on cyber space and provisions relating to punishment and prevention to the cybercrimes by discussing the judicial approaches which includes various prominent cases relating to cybercrimes and their roles in preventing cybercrimes in India. It highlights various problems relating to cyber space such as cyber stalking and cyber terrorism in length and tries to critically analyze the position of current statutes relating to cyber laws and evaluate as per current needs of the society in order to provide healthy suggestive measures which may prove helpful to curb this menace of cybercrimes.

1.3. AIM(S):

The primary aim of the present research is to critically analyze the concept of Crisis, Crisis management and Technological crisis in order to evaluate the preparedness of organizations in India and to expand the existing body of knowledge in the area of crisis management, by describing the technological crisis that can occur in IT companies. This study offers more insights towards the cause of occurrence of a particular Technological crisis. It contributes best in understanding that the traditional way of organizations to address crisis as communication by putting an ideal by articulating its fight against the cybercrimes and current cyber laws which works as supplement and but still it persists several grey areas which needs to be filled at earliest. Today's, technical experts believe that the efforts to let alone take the control of crisis situation can be often quite naïve. The inconsistencies and loopholes in researches clouds the perception towards occurrence of various Technological crisis and it ultimately results in missed opportunities to understand the subject in detail which also adversely impacts the performance of organizations. Crises are now seen as an inevitable part of any business or organisation, this present study aims at documenting the prevalent problems of technological Crisis that can occur across IT industry and then identifying the most prominent Crisis of such technology enabled organization in India.

Therefore, this study aims to classify the concept of uniform cyber law body which broadly includes other prospects such as intellectual property disputes resolutions and many more in order to avoid any collusions between them in future which results in hampering the growth of technology based organizations in India in order to boost them in managing future crisis more efficiently. Such logics are a foundation of participative management which is often seen as a philosophy best able to shape the structure of current cyber laws in India.

1.4. OBJECTIVE(S):

This paper tries to fulfil various objectives relating to organizational inclination towards its understanding of ‘crisis’ as a subject in order to identify the gap between knowledge and applicability in this area.

In the light of foregoing issues, the present study has targeted for the achievement of following broad set of objectives:

1. To identify and understand the prominent crisis prevailing in Indian Organizations.
2. To understand the concept of technological crisis faced by various technology enabled organizations in India.
3. To identify the factors responsible for the occurrence of such crisis in Indian Organizations.
4. To examine the theories relating to crisis management which can be applied by technology based Industries.
5. To understand the effects of such crisis on the work nature of the technology based organizations.
6. To understand the threat posed by combination of technological crisis and cybercrimes to the Indian organizations.
7. To identify the threats posed by technological crisis or any other crisis to the Indian organizations.
8. To describe the concept of cybercrimes with Indian perspective.
9. To discuss the nature, scope, characteristics and various classifications of cybercrimes with Indian perspective.
10. To understand various provisions relating to cyber offences punishable in India under Information Technology Act, 2000 and to check the judicial response towards cybercrimes.
11. To make suggestions for the improvement of technological crisis management process in India and to measures for the proper implementation of cyber laws in India.

1.5. SIGNIFICANCE OF THE STUDY:

The present study proves its significance primarily in the threefold manner, Firstly, it has explained the crisis as per Indian organization perspective by taking into the account of technological crisis on the basis of occurrence in such organization. Secondly, it has to its best efforts identified the major jurisprudence in order to evaluate such organizations/corporate readiness in the present times to manage such crisis in the most efficient manner. And thirdly, as the foremost part of the study, it attempts to identify the best possible crisis management models which can be applied by such organizations. This research tries in revitalizing their current crisis management strategies.

The proprietary business models of technology based organizations have been evolved through various technologies and its subsequent transformation through the internet enabled 'electronic data interchange' regarded as E-commerce, this paper tries to articulate the aspect of technology also includes e-commerce.

The preamble of the Information Technology Act 2000[1] enumerates that ....

"An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involves the use of alternatives to paper-based methods of communication and storage of information to facilitate electronic filing of documents with the Government agencies...."[2]

Bypassing the traditional methods by the latest technological processes, the business world is becoming more and more complex and in order to survive and in order to remain alive in the business competition, it is important one should adopt faster processing technological methods. The issue is not only how to boost up the quick process of technology in organizations but also how to overcome crisis among the technology based Indian organizations.

[1] Information Technology Act 2000 | Ministry of Electronics and Information Technology, Government of India, , https://meity.gov.in/content/information-technology-act-2000 (last visited Jan 14, 2020).
[2] *Ibid.*

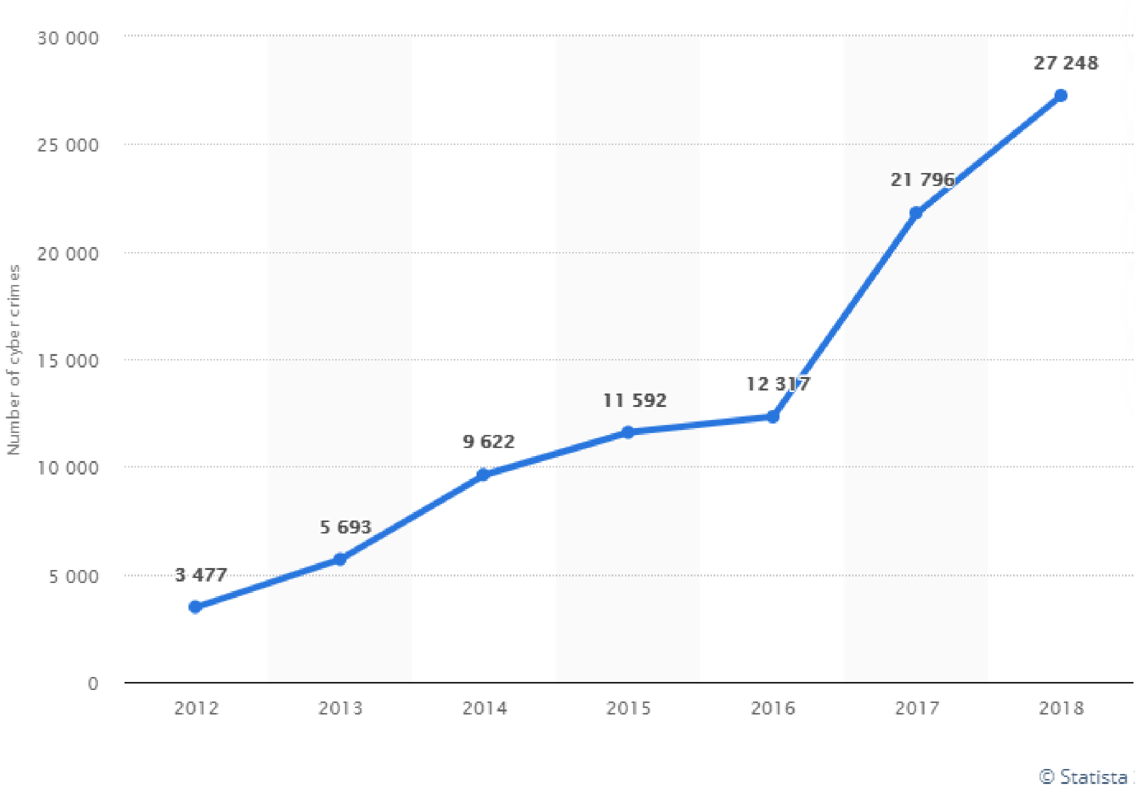


Figure 1.5.1: Number of cybercrimes in India from 2012-2018

(**Source**: Statista 2020)[3]

The above mentioned statistics clearly shows that the number of cases of cybercrimes in India are growing significantly each year and The single year in which the rate of cybercrimes *doubled* is in 2017 which makes the preventive measures of such cybercrimes in India even more suspicious and it is crucial to analyze the data collected along with this statistic to analyze the current position of technology based organizations in India to explore the adequacy of punishment provisions of present cyber laws in Indi and to analyze the technological crisis faced by such organizations.

The implementation of such technology with the existing law is still in question, by the observation near around the situation of Indian organizations, such technologies needs to be improved.

[3] India - number of cybercrimes 2018, STATISTA , https://www.statista.com/statistics/309435/india-cyber-crime-it-act/ (last visited Jan 14, 2020).

1.6. SCOPE AND LIMITATION:

The scope of this research includes two major divergent areas. This study explores the insights into understanding the crisis and its prevalent occurrence of technological crisis in the industries of India and moreover, identifies the prominent crisis management models and its importance for Indian organizations explained through the best possible jurisprudence relating to it. This study in its second phase has explored the factors, issues or causes leading to the cybercrimes, its historical aspect, identifying its jurisdiction and punishment and prevention provisions of cyber laws in India.

Moreover, to explore judicial approach towards cybercrimes along with comparative studies and critical analysis of collected data. The scope of this paper is limited to the study of following grounds:

1. Understanding the concept of crisis, technological crisis and best possible ways for the crisis management
2. Understanding the dangers that lurk in the technological crisis for the organizations in India.
3. Analyzing the sample taken from working staff of various technology enabled organizations in India.
4. Understanding the threat posed by combination of hacking, creating viruses and dark web and other aspects of cybercrimes.
5. Exploring the measures adopted by Indian government relating to internet management to reduce the cases relating to cyber space.
6. Understanding the punishment and prevention to the cybercrimes in India.
7. Understanding the judicial endeavors towards cybercrimes in India.
8. Exploring the comparative study of cybercrimes for finding the loopholes, if any.
9. Critically analyzing the concept of crisis and cybercrimes collectively as per present times.
10. Examining the present conditions of cyber laws in India and evaluating its adequacy in present times.

1.7. DETAILED LITERATURE REVIEW:

‘CRISIS’, the very word evokes the sense of insecurity. Indeed, it possess the strength to change our lives at professional as well as personal level. From domestic to world level, in today’s world the existence of crisis has becomes common in every form of organization.

In this study, a critical review of the literature concerning *first* facet of this research, published and unpublished is presented, since academicians, researchers and professionals have contributed very limited thought but provoking studies which come in the form of books and articles. Following are the previous research studies; those are related to the present research study.

1.7.1 TYPES OF CRISIS:

Crisis can be classified into several types. Some comes as surprise to management and some are the usual risk of business operations.

Several researchers have carried on their study to classify types of crisis.

Smith (1963)[4] has described seven different types of crisis-some external, some internal. These are crisis of growth; crisis stemming from the abdication of responsibility by the chief executive; crisis arising from loss of control over the organizational operations; crisis arises due to flaunts in laws; crisis of leadership; crisis of judgement; and finally crisis influenced by the competition:

Lippitt and Schmid (1967)[5] enumerated the stages of crises, that is crises which corporations attended while growing, from birth through youth and maturity. Superficially, these crises may look internal and external. But actually it grows from organizational birth pang and growing pains. They have identical critical concerns during each of these three stages and key crisis with respect to each critical concern.

[4] Corporations in Crisis by Smith, Richard Austin: Good Paperback | ThriftBooks, , https://www.abebooks.co.uk/Corporations-Crisis-Smith-Richard-Austin-Doubleday/30248280672/bd (last visited Apr 14, 2020).

[5] Crises in a Developing Organization, , https://hbr.org/1967/11/crises-in-a-developing-organization (last visited Apr 14, 2020).

Shiva Ramu (2000)[6] discussed several issues which leads to technological crisis. It involves the handling of hazardous material such as oil spills and yet another is related to market place, where corporation faces the common problem of product tampering and counterfeit activities. Sometimes, new product introduced have inbuilt risk involved in it and its damage may result in judicial dispute and also shatter the reputation of the corporation. Several types of cyberattacks may also leads to technical disaster situation to such corporations.

1.7.2 INDIVIDUAL REACTION TO CRISIS:

The optimum technology placed during work may vitally affect the organizational response towards crisis. Psychologists have studied the reactions of various human beings during the times of crisis and such reactions can be categorized as stress, shock or defensive retreats from the situation by the human beings. Many ties, acknowledgement of the crisis conditions and finally adaptation and change leads it to normalcy.

Cheryl Travers (1998)[7] has explained about the handling of stress during crisis conditions. She explained that corporate crisis is just people's perceptions rather than reality, the individual stress results from the situation dependent on how much an individual perceives it, she further emphasized on the point that effective crisis management is not primarily a set of tool which leads mechanisms to be implemented in organizations but a common mood and a set of action by the management which are not 'too emotionally' bounded.

1.7.3 GROUP REACTION TO CRISIS:

Due to its size, organizations are mainly managed by group of top level management rather than an individual, the response of group is also an important relevance to the organizational crisis. **Torrance (1958)**[8]**, Hambling (1958)**[9]**, Hare**

[6] S. SHIVA RAMU, CORPORATE CRISIS MANAGEMENT: CHALLENGES FOR SURVIVAL (2000).

[7] MICHAEL BLAND, COMMUNICATING OUT OF A CRISIS (2016).

[8] ROBERT J. ED STERNBERG, THE NATURE OF CREATIVITY: CONTEMPORARY PSYCHOLOGICAL PERSPECTIVES (1988).

[9] Robert L. Hamblin, *Leadership and Crises*, 21 SOCIOMETRY 322–335 (1958), https://www.jstor.org/stable/2785796 (last visited Mar 22, 2020).

(1962)[10] **and Shephard (1965)**[11] examined the stress reactions on small groups. They found an interesting discovery that has relevance to the organizations facing crisis is the greater influence attempts by informal leaders in a group faced with crisis and the greater acceptance of the authority of a leader in such a situation **(Torrence 1958**[12]**, Hambling 1958**[13]**)**. Groups tend to reject leaders who does not quickly resolve **Hambling (1958). Hare (1962, pg. 265**[14]**)** noted that: "Groups tend to respond to continuously stress like all living systems, first by a lag in response, then by an over compensatory response and finally by a catastrophic collapse of the system.

1.7.4 READINESS FOR CRISIS:

As organizations works as open system, they might not prepare themselves for future events. One cannot prepare for uncertain contingencies. However, the lack of foresight can be regarded as the lack of precautions. In this regard, several studies have been conducted.

According to **Mc Caskey (1974)**[15], directional plans are considered when there is high level of uncertainty and thus where flexibility is required in order to respond to the unexpected challenges. High uncertainty and unexpected shifts are basic elements of crisis situations.

Turner (1976)[16] implied towards the sequence of events associated with failure of the foresight as enumerated in the table 1.7.1.

Stages	Conditions
Stage I	Normal starting point:

[10] ALEXANDER PAUL HARE, HANDBOOK OF SMALL GROUP RESEARCH (1962).

[11] Robert T. Golembiewski & Stokes B. Carrigan, *Planned Change in Organization Style Based on the Laboratory Approach*, 15 ADMINISTRATIVE SCIENCE QUARTERLY 79–93 (1970), https://www.jstor.org/stable/2391191 (last visited Mar 22, 2020).

[12] STERNBERG, *supra* note 8.

[13] Hamblin, *supra* note 9.

[14] HARE, *supra* note 10.

[15] E. MUMFORD, VALUES, TECHNOLOGY AND WORK (2013).

[16] The Failure of Foresight in Crisis Management: A Secondary Analysis of The Mari Disaster, , https://www.researchgate.net/publication/249010918_The_Failure_of_Foresight_in_Crisis_Management_A_Secondary_Analysis_of_The_Mari_Disaster (last visited Mar 22, 2020).

	a) Initial culturally accepted belief about the world and its hazards. b) Associated precautionary norms set out in laws, codes of practice, folkways and mores.
Stage II	Incubation period: The acclamation of an unnoticed set of events which are at odds with affirmed beliefs regarding hazards and the norms for their avoidance.
Stage III	Precipitating the event: the event forces itself onto the attention and transforms general perceptions to stage II.
Stage IV	Onset: the immediate consequences of the collapse of cultural precautions becomes apparent.
Stage V	Rescue and Salvage: The first stage adjustment: the immediate post collapse situation is recognized in ad hoc adjustments which permits the work of rescue and salvage to be started.
Stage VI	Full cultural readjustment: An inquiry and assessments are carried out and beliefs and precautionary norms are adjusted to fit the newly gained understanding of the world.

Table 1.7.1: Events associated with the failure of Foresight

Source: Turner (1976) pg. 38[17]

A crisis or disaster happens mainly due to two primary factors, i.e., either inaccuracy or inadequacy in accepted norms and natures enumerated under the stages of above mentioned table. In the pluralistic societies, people have varied norms for values and perceptions regarding risks and conflicts do occur.

1.7.5 TECHNOLOGY CRISIS: SOCIAL PERSPECTIVE

A tremendous number of experts are heralding the era relating to the technological crisis: **Weick (1988)**[18] noted as being “... characterized by low

[17] *Ibid.*

[18] Enacted Sensemaking in Crisis Situations - Talking About Organizations Podcast, , https://www.talkingaboutorganizations.com/e26/ (last visited Mar 22, 2020).

probability/high chronological events that threaten the most fundamental goal of an organization...”.

Shrivastava et al. (1988)[19] recognized breakdown of technological process as being organizationally based, socio-technical disasters which causes heavy damage and social disruption, involve multiple stakeholders and unfold through complex, technological¸ organizational and social processes.

Smith (1990)[20] explained the ‘7C’s’model of crisis management in which he enumerated the organizational elements which can be combined together for the purpose of examining the prevalent technology crisis. These ‘7C’s’ are crucial for reducing the crisis proneness inherent with the core beliefs and values of the organization and to enhance the ability of organization to avoid and/or efficiently manage the socio-technical disaster crisis.

1.7.6 CRISIS MANAGEMENT:

According to the ideology of **Shrivastava (1988)**[21]**,** this study of management still lacks the adequate integration between one another and still possess very large area to work on. Specifically, organizational crises inherently are phenomena for which psychological, sociopolitical and technological structural issues act as integral forces in their creation and management **(Pauchant and Douville, 1994)**[22]. The study of crisis management includes multiple disciplines and scholars believes that must be studied and managed using systems approach **(Bewonder and Linstone, 1987)**[23]. In other words, scholar believes that psychological, sociopolitical and technological structural issues should be

[19] UNDERSTANDING INDUSTRIAL CRISES[1] - Shrivastava - 1988 - Journal of Management Studies - Wiley Online Library, , https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1467-6486.1988.tb00038.x (last visited Mar 22, 2020).

[20] The three phase model of Crisis, , https://www.ukessays.com/essays/management/the-three-phase-model-of-crisis-management-essay.php (last visited Mar 22, 2020).

[21] UNDERSTANDING INDUSTRIAL CRISES[1] - Shrivastava - 1988 - Journal of Management Studies - Wiley Online Library, *supra* note 19.

[22] Pauchant T and Douville R 1993 Recent research in crisis management A study of | Course Hero, , https://www.coursehero.com/file/p3o1ja8/Pauchant-T-and-Douville-R-1993-Recent-research-in-crisis-management-A-study-of/ (last visited Mar 23, 2020).

[23] B Bowonder 1987 An analysis of the Bhopal accident Project 168 | Course Hero, , https://www.coursehero.com/file/p1m8m35j/B-Bowonder-1987-An-analysis-of-the-Bhopal-accident-Project-Appraisal-23-157-168/ (last visited Mar 23, 2020).

explicitly considered and due recognized while studying and managing organizational crisis.

Further, a critical review on the literature concerning *second* facet of this research, published as well as an unpublished is presented. Following are the previous research studies; those are related to the present research study.

1.7.7 CYBER CRIMES:

In present times, the problem of cybercrimes is getting common in India due to consistent rise in its cases. It is pertinent to look into the present studies along with sample collected in order to critically analyze it for the purpose of preventing it in future, especially, with the perspective of Indian organizations.

G. Rathinasabapathy (2005)[24], concentrated on rapid raise in cybercrimes. Cybercrime which is also known as 'Internet crimes' or 'Computer crimes' is any criminal activity that uses a computer either as an instrument, target or a means for perpetuating further crimes or offences or contraventions under any law. Major cybercrimes reported in India are denial of services, defacement of web sites, spam, computer virus and worms, pornography, cybersquatting, cyber stalking and phishing. Further, most of the big libraries especially academic libraries are now have various kinds of networks like Local Area Network, Wide Area Network, etc. Library services are also being offered in networked digital environment. The author has also briefed about cybercrimes, its relevance and various ways to prevent cybercrimes. Computer-related crime, in particular cybercrime such as phishing and its progeny, require a different solution due to the non-terrestrial and non-territorial nature of electronic transactions. In order to fight such crimes effectively, a strong and robust international regime is needed; and one that is as far as possible harmonized. In order for there to be an effective global system to deal with the problem of computer-related crimes, there must be a multifaceted and multipronged approach using a combination of both legally coercive and non-legal measures.

[24] G. Rathinasabapathy & L. Rajendran, *RFID Technology and Library Security: Emerging Challenges*, 1 JOURNAL OF LIBRARY, INFORMATION AND COMMUNICATION TECHNOLOGY 34–43 (2015).

‘Prevention is better than cure’ is not only meant for human health but for computers as well. It is always better to take necessary steps to prevent cybercrimes. Cybercrimes in India are slowly evolving from a simple e-mail crime to more serious Crimes like hacking and source code theft. It is a known fact that given the unrestricted number of free Web sites, the Internet is undeniably open to exploitation, cases of spam, hacking, cyber stalking and email fraud are rampant and, although cybercrimes cells have been set up in major cities, the problem is that most cases remain unreported due to a lack of awareness.

Jerry Kang (2000)[25], thought that, most inquiries into race and cyberspace have focused on the "digital divide" - whether racial minorities have access to advanced computing communication technologies. Can cyberspace change the way that race functions in American society? He argues that cyberspace can disrupt racial schemas because it alters the architecture of both identity presentation and social interaction. Thus, cyberspace presents society with three design options: abolition, integration, and transmutation. After analyzing each option's merits, Professor Kang concludes that society need not adopt a single, uniform design strategy for all of cyberspace. Instead, society can embrace a policy of digital diversification, which explicitly zones different cyber spaces according to different racial environments. Although cyberspace is no panacea for the racial conflicts and inequality that persist, it offers new possibilities for furthering racial justice that should not be wasted.

1.7.8 JURISDICTION TO CYBERCRIMES:

Abraham D. Sofaer, Seymour E. Goodman, Mariano-Florentino Cuellar, Ekaterina A. Drozdova, David D. Elliott, Gregory D. Grove, Stephen J. Lukasik, Tonya L. Putnam, George D. Wilson (August 2000)[26], in their paper entitled as *“International Convention on Cyber Crime and Terrorism”*, they

[25] JERRY KANG, *Cyber-Race* (2004), https://papers.ssrn.com/abstract=631725 (last visited Mar 26, 2020).

[26] Abraham D. Sofaer & Seymour D. Goodman, *A Proposal for an International Convention on Cyber-Crime and Terrorism* (2000), https://www.semanticscholar.org/paper/A-Proposal-for-an-International-Convention-on-and-Sofaer-Goodman/0911d08990a8b59f90046c49b82cad2c5174e9d3 (last visited Mar 26, 2020).

conclude that, the information infrastructure is increasingly under attack by cyber criminals. The number, cost, and sophistication of attacks are increasing at alarming rates. Worldwide aggregate annual damage from attacks is now measured in billions of U.S. dollars. Attacks threaten the substantial and growing reliance of commerce, governments, and the public upon the information infrastructure to conduct business, carry messages, and process information. Measures thus far adopted by the private and public sectors have not provided an adequate level of security. Investigations have been slow and difficult to coordinate. Some attacks are from States that lack adequate laws governing deliberate destructive conduct. Cybercrime is quintessentially transnational, and will often involve jurisdictional assertions of multiple States. A clear consensus emerged that greater international cooperation is required, and considerable agreement that a multilateral treaty focuses on criminal abuse of cyber systems would help build the necessary cooperative framework. This monograph summarizes and presents the Stanford Draft International Convention to Enhance Security from Cyber Crime and Terrorism and commentary on die Draft. The Draft acknowledges and builds upon the draft Convention on Cyber Crime proposed by the Council of Europe.

Neal Kumar Katyal (April 2001)[27], thought that, the ILoveYou computer worm and the denial of service attacks on Yahoo, eBay, and ETrade, suggest that a new form of crime is emerging: cybercrime, causing more than $11 billion in losses. This paper asks how cybercrime is best deterred. It identifies five constraints on crime - legal sanctions, monetary perpetration cost, social norms, architecture, and physical risks - and explains how each of these constraints may be reduced by committing crime in cyberspace. Cybercrime requires fewer resources and less investment to cause a given level of harm, the law might want to use approaches that differ somewhat from those in real space. Criminal law must be concerned not only with punishing crime ex post, but with creating ex ante barriers to inexpensive ways of carrying out criminal activity. Some government barriers, however, will create deadweight losses. The paper advocates the use of sentencing enhancements

[27] Criminal Law in Cyberspace by Neal Kumar Katyal :: SSRN, , https://papers.ssrn.com/sol3/papers.cfm?abstract_id=249030 (last visited Mar 26, 2020).

as tools that surgically target bad acts. Sentencing enhancements have received relatively little attention in the academic literature; this Article attempts to fill that gap. Cyberspace also adds additional parties to the traditional perpetrator-victim scenario of crime. Law should impose modest responsibilities on third parties because doing so promotes cost deterrence and capitalizes on what Reinier Kraakman has called gatekeeper liability. Burden-shifting must not, however, sacrifice the value of interconnectivity and network effects

Susan W Brenner (April 2002)[28], in their paper entitled as "Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law" they thought that, the development of the Internet and the proliferation of computer technology has created new opportunities for those who would engage in illegal activity. The rise of technology and online communication has not only produced a dramatic increase in the incidence of criminal activity, it has also resulted in the emergence of what appear to be some new varieties of criminal activity. Criminal activity poses challenges for legal systems, as well as for law enforcement. Legal tools include an arsenal of well-defined cybercrime offenses for use in prosecuting cyber criminals and procedural rules governing evidence-gathering and investigation. Cybercrime is often transnational in character; offenders can take advantage of gaps in existing law to avoid apprehension and/or prosecution. It is, therefore, important that every legal system take measures to ensure that its penal and procedural law is adequate to meet the challenges posed by cybercrimes. The primary focus of the article is on penal laws simply because there tends to be more consistency in the way countries define criminal offenses than in die area of procedural law. In order to maintain the level of internal stability a nation must enjoy to survive and prosper, each country must have penal laws that protect the safety of individuals ("crimes against persons"), that preserve the integrity of at least certain types of property ("crimes against property"), that prohibit interference with the legal system ("crimes against the administration of justice"), and that proscribe attacks on the government

[28] Approaches to Cybercrime Jurisdiction, , RESEARCHGATE , https://www.researchgate.net/publication/228198888_Approaches_to_Cybercrime_Jurisdiction (last visited Mar 26, 2020).

("crimes against the state"). It is, however, not possible to postulate the same level of generic consistency with regard to procedural law; although there are empirical constancies in the procedures law enforcement uses when investigating and prosecuting crimes, nations vary widely in the legal constraints they place on these processes.

R. Benjamin, B. Gladman and B. Randell (2014)[29]: Protecting IT Systems from Cyber Crime Large-scale commercial, industrial and financial operations are becoming ever more interdependent, and ever more dependent on IT. At the same time, the rapidly growing interconnectivity of IT systems, and the convergence of their technology towards industry-standard hardware and software components and sub-systems, renders these IT systems increasingly vulnerable to malicious attack. This paper is aimed particularly at readers concerned with major systems employed in medium to large commercial or industrial enterprises. It examines the nature and significance of the various potential attacks, and surveys the defence options available. It concludes that IT owners need to think of the threat in more global terms, and to give a new focus and priority to their defence. Prompt action can ensure a major improvement in IT resilience at a modest marginal cost, both in terms of finance and in terms of normal IT operation.

Talwant Singh (2004)[30]: Sessions Judge, Delhi in his article "Cyber Law & Information Technology" states that what were the problem and technicality for the implementation of cyber law. This issue is a core part of our research. Actually the theme to do research in this area came to my mind after reading this article. This article shows that how difficult it is to implement the cyber law in practicality? Success in any field of human activity leads to crime that needs mechanisms to control it. Legal provisions should provide assurance to users, empowerment to law enforcement agencies and deterrence to criminals. The law is as stringent as its enforcement. Crime is no longer limited to space, time or a group of people. Cyber space creates moral, civil and criminal wrongs. It has now given a new way to

[29] BHATTATHIRIPAD POLPAYA VINOD, JUDICIARY-FRIENDLY FORENSICS OF SOFTWARE COPYRIGHT INFRINGEMENT (2014).

[30] Talwant Singh, *Cyber law & information technology* (09:13:47 UTC), https://www.slideshare.net/talwant/cyber-law-information-technology (last visited Mar 26, 2020).

express criminal tendencies. Back in 1990, less than 100,000 people were able to log on to the Internet worldwide. Now around 500 million people are hooked up to surf the net around the globe. Until recently, many information technology (IT) professionals lacked awareness of and interest in the cybercrime phenomenon. In many cases, law enforcement officers lack the tools needed to tackle the problem; old laws didn't quite fit the crimes being committed, new laws hadn't quite caught up to the reality of what was happening, and there were very few court precedents to look to for guidance. Furthermore, a debate over privacy issues hampers the ability of enforcement agents to gather the evidence needed to prosecute these new cases. Finally, there was a certain amount of antipathy—or at the least, distrust—between the two most important players in any effective fight against cybercrime: law enforcement agencies and computer professionals. Yet, close cooperation between the two is crucial if we are to control the cybercrime problem and make the Internet a safe "place" for its users. Law enforcement personnel understand the criminal mindset and know the basics of gathering evidence and bringing offenders to justice. IT personnel understand computers and networks, how they work, and how to track down information on them. Each has half of the key to defeating the cybercriminal. IT professionals need good definitions of cybercrime in order to know when (and what) to report to police, but law enforcement agencies must have statutory definitions of specific crimes in order to charge a criminal with an offence. The first step in specifically defining individual cybercrimes is to sort all the acts that can be considered cybercrimes into organized categories.

Amit Nayak (2004)[31]: Understanding Cyber Crime Movements in Asia. The author focuses on the definition of cybercrime that IT professional should know when to report to police, also law enforcement agencies must have statutory definitions of specific crimes in order to charge a criminal with an offence. The author says that first step in specifically defining individual cybercrimes is to sort all the acts that can be considered cybercrime into organized categories. Due to the global connectivity because of BPO, multimillion transactions can be conducted.

[31] Amit NAYAK | Charotar University of Science and Technology, Anand | CHARUSAT | Department of Information Technology, , https://www.researchgate.net/profile/Amit_Nayak3 (last visited Mar 27, 2020).

The easy access to the internet and a booming market for related new communications devices have changed the way we spend, our leisure time and the way we do business. In today's world ways in which criminals commit crimes is also changing. Universal digital accessibility opens up new opportunities for the unscrupulous. Millions of dollars are lost to computer-savvy criminals by both businesses and consumers. Worse, computers and networks can be used to harass victims or set them up for violent attacks-even to coordinate and carry out terrorist activities that threaten us all. Unfortunately, in many cases law enforcement agencies have lagged behind these criminals, lacking the technology and the trained personnel to address this new and growing threat, which has been aptly, termed cybercrime. The author says that many information technology (IT) professionals lacked awareness of and interest in the cybercrime phenomenon. In many cases, law enforcement officers have lacked the tools needed to tackle the problem; old laws didn't quite fit the crimes being committed, new laws hadn't quite caught up to the reality of what was happening, and there were very few court precedents to look to for guidance. But even then close cooperation between the two is crucial if we are to control the cybercrime problem and make the Internet a safe "place" for its users. The author, Quantify the Crisis as Cybercrime. It sounds exotic, the stuff of which futuristic science fiction novels are made. However, law enforcement officers, network administrators, and others who deal with crime and/or cyberspace are discovering that the future is now, and cybercrime is a big and growing problem. He then has given various examples such as According to the Internet Fraud. Complaint Center (IFCC), a partnership between the Federal Bureau of Investigation (FBI) and die National White Collar Crime Center, between May 2000 and May 2001, its first year of operation, the IFCC Web site received 30,503 complaints of Internet fraud.

Dr. Farooq Ahmad (2004)[32]: The famous *Cyber Law in India (Law On Internet)* book written by Dr. Farooq Ahmad, is a good book to understand all tiny

[32] CYBER LÄW IN INDIA. (Law on Internet) Dr. Farooq Ahmad Reader, Department of Law University of Kashmir, Srinagar - PDF Free Download, , https://docplayer.net/10432956-Cyber-law-in-india-law-on-internet-dr-farooq-ahmad-reader-department-of-law-university-of-kashmir-srinagar.html (last visited Mar 27, 2020).

concepts required for this research. It has emphasized on implications of the Cyber Law in general. Information Technology solutions have paved a way to a new world of internet, business networking and e-banking, budding as a solution to reduce costs, change the sophisticated economic affairs to easier, speedy, efficient, and time saving method of transactions. Internet has emerged as a blessing for the present pace of life but at the same time also resulted in various threats to the consumers and other institutions for which it's proved to be most beneficial. Various criminals like hackers, crackers have bear able to pave their way to interfere with the internet accounts through various techniques like hacking the Domain Name Server (DNS), Internet Provider's (IP) address, spoofing, phishing, internet phishing etc. and have been successful in gaining "unauthorized access" to the user's computer system and stolen useful data to gain huge profits from their accounts.

Intentional use of information technology by cyber terrorists for producing destructive and harmful effects to tangible and intangible property of others is called "cybercrime". Cybercrime is clearly an international problem with no national boundaries. Hacking attacks can be launched from any comer of the world without any fear of being traced or prosecuted easily. Cyber terrorist can collapse the economic structure of a country from a place where the country might not have any arrangements like "extradition treaty" to deal with that criminal. The only safeguard would be better technology to combat. Such technology already evolved and known to the Hackers, but that still has threat of being taken over by the intellect computer criminals.

1.7.9 FINANCE RELATED CYBERCRIMES:

Brian Cashell, William D. Jackson, Mark Jickling, and Baird Webel, Government and Finance Division (April, 2004)[33], in this paper authors describe the Information security - the safeguarding of computer systems and the integrity, confidentiality, and availability of the data they contain - has long been recognized

[33] Brian Cashell et al., *The Economic Impact of Cyber-Attacks* 45.

as a critical national policy issue. Author has explained the two current trends, first, the integration of computers into more and more aspects of modem life continues. Second, cyber-attacks, or breaches of information security, appear to be increasing in frequency, and few observers are willing to ignore the possibility that future attacks could have much more severe consequences than what has been observed to date. Though cyberattacks have been relatively limited in scope Individual firms, may have suffered significant losses as a result of past attacks. Author also discussed the economic effect of cyberattacks on stock process. In theory, the price of a company's stock is primarily determined by the present discounted value of the cash flows expected to result from that firm's output That cash flow is what contributes to the wealth of the stockholders, either in the form of dividends or in the expansion of the firm's stock of productive capital. Author said that any event that changes investors' expectations about that future stream of income is likely to affect the price of the stock. Author has described the types of attacks according to the business is affected. As long as any cyber- attack is limited in scope and short-lived it is likely that macroeconomic consequences will be small. But the ability to recover quickly is important, since the length of time computers are affected is an important determinant of the costs.

Peter Grabosky (2005)[34]: "*The Global and Regional Cyber Crime Problem*". This paper provides an overview of computer-related crime. Eleven varieties of crimes are considered: theft of services; communications in furtherance of criminal conspiracies; information piracy and forgery, the dissemination of offensive materials; cyberstalking; extortion; electronic money laundering; electronic vandalism and terrorism; sales and investment fraud; illegal interception; and electronic funds transfer fraud. The most appropriate strategies for the control of computer-related crime entails a mixture of law enforcement, technological and market-based solutions. It is argued that in some contexts, the market place may be able to provide more efficient solutions to the problems of computer-related crime than state interventions. This paper discusses current and emerging forms of

[34] Peter Grabosky, *The Global and Regional Cyber Crime Problem*, PROCEEDINGS OF THE ASIA CYBER CRIME SUMMIT 22–42 (2001).

computer-related illegality. It reviews eleven generic forms of illegality involving information systems as instruments or as targets of crime. It will also discuss issues arising from the global reach of information systems. It is trite to describe the ways in which computers have, figuratively speaking, made the world a smaller place. The corresponding potential for trans-jurisdictional offending will pose formidable challenges to law enforcement. For some crimes, this will necessitate a search for alternative solutions. Computer-related illegality lies beyond the capacity of contemporary law enforcement and regulatory agencies alone to control, and that security in cyberspace will depend on the efforts of a wide range of institutions. Trans-national crime of a more conventional nature has proved to be a very difficult challenge for law enforcement. Computer-related crime poses even greater challenges. There may be differences between jurisdictions about whether or not the activity in question has occurred at all, whether it is criminal, who has committed it, who should investigate it and who should adjudicate and punish it Moreover, there is a fundamental tension between the deregulatory imperative which characterizes the world's advanced economies and the desire to control some of the darker comers of cyberspace.

1.7.10 OTHER STUDIES RELATED TO CYBERCRIMES:

Professor Soumyo D. Moitra (2006)[35]: "Modeling Cybercrime for Internet Risk Management" Kolkata, India. In his published book author has concentrated on the cybercrime. Internet crime is considered as a cybercrime. In this, cybercrime of basic modeling & its benefits are outlined. National policymakers & regional blocks have considered & to implement number of measures to control cybercrime. However, many policy making are based on media report, public reaction & adhoc data. Most of the surveys till date have serious methodological limitations. The author has focused on nature of cybercrime also. There are major gaps in our knowledge, such as the crime commission rate of malicious hackers, the relationship between cybercrime experienced at a site and the characteristics of that site or the detection and reporting rates of victim sites. Author has also discussed

[35] Soumyo D. Moitra, *Modelling Cybercrime for Internet Risk Management* (2007).

about secondary date. In recent years, a considerable number of reports have been published which present results of surveys or collected information on alleged cybercrimes. Internet risk management and the design of future surveys. It is important that models are developed first to guide the empirical research so that more meaningful survey instruments can be constructed. Then we shall be able to collect data that would provide accurate insights into the cybercrime process and yield results that would be useful to further the knowledge of cybercrime.

Florence Tushabe, and Venansius Baryamureeba (2007)[36]: "Cyber Crime in Uganda: Myth or Reality?" The author has focused on cybercrimes in Uganda. There is a general feeling that Internet crime is an advanced type of crime that has not yet infiltrated developing countries like Uganda. The author conducted an independent research to ascertain whether cybercrimes have affected people in Uganda and if so, to discover where they are reported? Internet users in Uganda have not been victims or perpetrators of Internet crimes? Informal and scanty reports about computer crime in Africa and in Uganda particularly result in a misconception that those crimes do not feature there. They include crimes like cyber terrorism, intellectual property infringement, hacking, industrial espionage, on-line child exploitation, Internet usage policy abuses, illegal purchase of goods, sexual assault, internet fraud, software piracy, viruses, impersonation and many more. Authors study has revealed that cybercrime is silent but common even in the developing countries like Uganda. As much as 90% of Internet users in Uganda have suffered losses causal by Internet crimes. It is hard to convict cyber criminals because of two major reasons. Firstly, few countries have enacted e-laws and the existing ones are not sufficient in convicting culprits because of jurisdiction anomalies especially when the investigation transcends international borders. Secondly, obtaining evidence of computer crime that would stand in courts of law is lacking in many countries since the field of computer forensics is still relatively new and lacks sufficient literature and expertise

[36] Florence Tushabe & Venansius Baryamureeba, *Cyber Crime in Uganda: Myth or Reality?* (2005).

R. K, Chaubey (2009)[37]: Cybercrime is the latest type of crime which affects many people. It refers to criminal activity taking place in computer networks, knowingly or intentionally, access without pennission, alters, damage, deletes and destroys the database available on the computer or network. It also includes the access without pennission to the database or programme of a computer or network in order to devise or execute any unlawful scheme or wrongfully control or obtain money, property or data. It poses the biggest challenge for police, prosecutors and legislators.

Justice Yatindra Singh (2012)[38]: The proper analysis of Cyber Laws, the author lucidly explains the science behind the technology in order to sort out the legal issues. The internet has introduced another technology known as webcasting or internet broadcasting which involves streaming of audio/video on internet called internet radio. These are retransmission of over the air broadcasts through internet. The internet has brought forward a new class of persons, known as intermediaries, who provide physical facilities to transmit or route the information, also known as Internet Service Providers. The study is an asset to companies dealing in computer software or providing software solutions, web page providers, Internet service providers, Banks, Insurance companies and other bodies providing online services, government departments implementing information technology, police officials dealing with investigation of cyber-crimes, teachers, students, lawyers and judges.

Vakul Sharma (2004)[39]: The study comprises of numerous illustrations, concept notes and examples make the subject interesting and comprehensible. It attempts to interpret the true legislative intent behind the Act by referring to and applying the Supreme Court judgments for better assimilation and understanding of its various provisions relating to cybercrime.

The author has tried to assimilate the thoughts of Judges, Lawyers, Civil Servants, Police Officers, Technocrats and Students whom he met during his public

[37] R. K. CHAUBEY, AN INTRODUCTION TO CYBER CRIME AND CYBER LAW (2009).

[38] CYBER LAWS, (2016).

[39] Vivek Dhupdale, *Cyber Crime and Challenges Ahead*, 2 IN THE INDIAN JOURNAL OF LAW AND JUSTICE, DEPARTMENT OF LAW, UNIVERSITY OF NORTH BENGAL, DARJEELING, WEST BENGAL 102–114 (2011).

lectures, discussions, workshops, seminar across the length and breadth of the country over the past many years.

The critical appraisal of powers and functions of the Cyber Regulatory Appellate Tribunal, Controller of Certifying Authorities, Adjudicating Officers and Police Officers under the Information Technology Act has been attempted.

Nandan Kamath (2008)[40]: The Internet has emerged as a medium with immense potential, posing many new and interesting challenges. There have been many attempts to regulate and control this medium, especially through the laws and regulations. This exciting publication explores the various aspects of cyber law and cyber regulations, taking the reader through a multitude of legal and policy issues that the Information Age poses. Topics covered in this book range from evidentiary aspects and digital signatures to intellectual property concerns such as copyright liability and rights in domain names; from cybercrime and cyber porn to the regulation of free speech on the Net and the right to privacy. A new chapter on Cases on Computers, Internet, e-mail etc. have been added. Employing a comparative law approach, this book, in its fourth edition, not only takes into consideration the changes brought about by the Information Technology Act of 2000, but also contains the latest developments along with a comprehensive guide to this legislation. Being wide-ranging as well as in-depth in its coverage of Indian Cyber law, this publication is a must-read for judges, lawyers, Policy makers, researchers, investigators and students as it is for anyone who would like to keep abreast of new developments in the legal system, concerning Information Technology.

Pavan Duggal (2013)[41]: The emerging developments in cyber law along with the dark side of Internet and the world wide web and its consequent legal consequences have made the thing interesting in understanding the cybercrime and its control mechanism. Cyber law is a phenomenon has evolved in our own lifetimes. In the last decade and a half, huge developments have taken place which

[40] LAW RELATING TO COMPUTER, INTERNET AND E-COMMERCE: A GUIDE TO CYBERLAWS, (2004).

[41] Indian Cyber Law Developments 2013, , ECONOMIC TIMES BLOG (2013), https://economictimes.indiatimes.com/blogs/Cyberlawsintodaystimes/indian-cyber-law-developments-2013/ (last visited Mar 28, 2020).

impacts every user of a computer, computer resource and communication device. Cyber law is one of the latest and most complex disciplines of legal jurisprudence.

Rodney D. Ryder (2001)[42]: in book "*Guide to Cyber Laws (Information Technology Act, 2000, E-Commerce, Data Protection and the Internet)*" has comprehensively discussed the provisions of the Information Technology Act, 2000 which is further amended in 2008. That's why his book named as a guide to cyber laws which includes all the provisions relating to information technology, e-commerce, data protection and the internet with special reference to Information Technology Act, 2000. He has stated some weaknesses of the above said Act and also suggested some measures for removing such weaknesses and curing the offences relating to information technology, e-commerce, data and the internet which we have called as cybercrimes. He has properly analyzed all the relevant provisions of cyber laws in order to sort out the legal issues by explaining the science behind the new emerging technology. He has mentioned the concept of digital signature, electronic signature and all the relevant provisions relating to it including with procedure of authentication and recognition of it. He has also through light on the electronic governance with relevant provisions given under the Information Technology Act, 2000 as amended by Amendment Act, 2008. He has also mentioned all the cyber offences recognized and punishable under Information Technology Act, 2000 as amended by Amendment Act, 2008.

Anirudh Rastogi (2014)[43]: in book "*Cyber Law- Law of Information Technology and Internet*" has explained the meaning, nature and scope of cybercrimes and cyber offences punishable under the Information Technology Act, 2000 as Amended by Amendment Act, 2008. According to him, cybercrime encompasses any crime which involves any computer system or network, where such system or network is a target of the crime, a tool of the crime or as a repository of evidence related to crime. The main concern of his work is to address and to point out that the scope of the cybercrime is itself changing rapidly with the

[42] RODNEY D. RYDER, GUIDE TO CYBER LAWS : (INFORMATION TECHNOLOGY ACT, 2000, E-COMMERCE, DATA PROTECTION & THE INTERNET) (2001).

[43] CYBER LAW-LAW OF INFORMATION TECHNOLOGY AND INTERNET, (Second edition ed. 2014).

evolution of the information technology and the scale at which it is used, or often misused. He has also discussed the concept of intellectual property rights i.e. trademarks, copyrights, patents and domain name dispute on cyber space. He has mentioned the concept of digital signature, electronic signature and all the relevant provisions relating to it including with procedure of authentication and recognition of it. He has also through light on the electronic governance with relevant provisions given under the Information Technology Act, 2000 as amended by Amendment Act, 2008. He has made an attempt to analyses the cyber laws governing the jurisdiction both in civil and criminal cases.

Vivek Sood (2008)[44] in book "*Cyber Law Simplified*" has discussed about all the legal issues relating to cybercrimes, electronic evidence, its relevancy, investigation procedure for dealing cybercrimes etc. He has made the harmonious analysis of key provisions of the Information Technology Act, 2000. He has explained all the concepts in a simple way which would provide us the clear understanding of all the areas like business, commerce, tax, information technology and human resources etc. His book suggested solutions for various cyber legal problems. He has given the suggestion for the application of various strategies to combat cybercrimes and how to investigate these crimes. He also suggested for enhancing the cooperation between the nation and the law enforcement agencies for bringing the cyber criminals before law. His work successfully made an effort to facilitate the legal planning, decision making and cyber legal compliance in the cyber world. Moreover, he also stressed on the implementation of the extradition treaties in the cyber age. While discussing about the importance of technology, he has stated that since cybercrimes are technology based, so the security technology is the best answer to these crimes. He has also concluded that protect yourself is best mantra against cybercrimes.

[44] Cyber Law Simplified - Vivek Sood - Google Books, , https://books.google.com.pk/books?id=Wxk89dMjxIQC&printsec=frontcover#v=onepage&q&f=false (last visited Mar 28, 2020).

Dr. Vishwanath Paranjape (2010)[45]: in book "*Legal Dimensions of cybercrimes and Preventive Laws with Special Reference to India*" has stated that cybercrime is emerged as a global issue with the rapid development of internet and computer technology. He has discussed the various legal dimensions and Indian legislative measures for the prevention of cybercrimes. He has comprehensively mentioned the various conventions, conferences, summits etc. on cybercrimes held at national and international level. His book is worked as the comprehensive treatise on the law relating to cybercrimes and the preventive strategies to check this global menace. In his book he has made efforts to investigate and find out the relevant legislation and judicial trends towards cybercrimes and cyber criminals. He has also traced the origin of these types of crimes and its impact on the criminal justice administration system. He has suggested that there is a need of international cooperation between nations for curbing the cybercrimes.

V.D. Dudeja (2002): in book "*Cyber Crime and the Law*" has discussed the new type of crime which has come into existence due to the use of information technology, computer, internet and its advancement. He has highlighted the various concepts relating to cybercrime and all the relevant provisions of cyber laws. He has emphasized on the significance of freedom of expression with reference to use of internet and suggested that some reasonable restrictions can also be put on the use of computers and internet in the interests of privacy and security purposes so that the law can recognize the computer as a 'weapon of offence' as well as a 'victim of offence.' He has suggested various measures for the prevention of these types of crime which are increasing day-by-day in the cyber world.

[45] Legal Dimensions of Cyber Crimes and Preventive Laws with Special Reference to India- Buy online now at Jain Book Agency, Delhi based book store., , https://www.jainbookagency.com/newdetails.aspx?id=78091 (last visited Mar 28, 2020).

1.8. RESEARCH QUESTIONS:

This paper tries to study and critically analyze the following research questions along with the questionnaire for the collection of samples, enumerated as:

a) Is there any form of crisis prevalent which is currently faced by Indian Organizations?
b) Whether the problems of technological crisis are present in the Indian Organizations?
c) Whether the conditions of crisis are being managed efficiently by the Indian Organizations?
d) Whether the problems of cybercrimes are being faced by the Indian organizations?
e) Whether the present cyber laws are sufficient to deal with the problems of crimes relating to cyber space?
f) Whether any suggestive measures can be taken to deal with the cases of cybercrimes in India?

1.9. HYPOTHESIS:

Based on the below mentioned hypotheses, this paper analyzes the facts and concepts of crisis, technological crisis, crisis management and cybercrimes in India, along with their relationship in the context of the organizations of India.

The hypotheses are pointed out on the basis of scope, concepts, significance and historical aspects of the topic and validity of which is to be tested from the survey conducted for the collection of appropriate data from the Indian organizations using technology in any major form are mentioned below as:

a. Crisis, in its various forms affecting the work process of technology enabled organizations in India. Technological crisis or other organizational crisis directly influence the efficacy of technology enabled organizations in India. Crisis Management models are important to increase the efficacy of technology enabled organizations in India. Knowledge accessibly influence the efficacy of the Crisis

Management Activities of technology enabled organizations in India. Technology learning capacity and its adaptability directly influence the efficacy of technology enabled organizations in India

b. Cybercrimes are socio-legal crimes and there are still various difficulties in the investigation. There is a need of a sufficient cyber legislation in order to curb this menace. Internet is becoming more dangerous for children although India is adopting various strategies to in combating with cybercrimes. Despite of safeguards, country is facing cybercrimes due to poor machinery and problem of laws, jurisdictions and awareness.

Therefore, the research hypotheses as formulated above will help the research in obtaining relevant and useful informations associated with the topic under concern. However, for achieving this purpose, it is important to carry out a thorough and detailed investigation on all the major aspects of Indian organizational crisis management and cybercrimes in order to understand its significance in a proper manner.

1.10. RESEARCH METHODOLOGY:

This chapter elaborates the research framework adopted for the study. It explicates the research objectives and dimensions of the study along with the set of methodologies implemented to attain each objective. It further looks at the measures followed to select the sample, collect data and different tools and techniques applied for analysis of the data.

1.10.1 METHODOLOGY SELECTED:

Research entails a systemized approach to extricate things that are unexplained or unexplored. One of the most holistic definitions given for Research refers to a plan, structure and strategy of investigation comprehended to obtain answers to research questions or problems. A plan is an absolute design or agenda of the research. It consists of a basic outline of what the researcher will do starting from identifying and writing the purpose or objective of the study and thereby listing the operational implications of the final analysis of data.

The present study comprises both Empirical and Doctrinal study. Empirical study is carried out when a new area is being explored or when very little is known about an area of interest. To explore the full nature of the observable fact and other related factors empirical study is adopted. The present study is doctrinal in nature in the first stage and empirical in second stage as the researcher started with classifying insights into the research topic and comprehending the problem situation or statement in order to frame a conceptual distinction against work done by others in the same area.

During the initial phase of exploration, it was observed that there was hardly any research carried out that explored the problem of Technological Crisis in the technology enabled Industries in India. As a conceptual distinction, the present study examines the construct of occurrence of various forms of Crisis and evaluation of such crisis through management tools, on the basis of frequency and intensity of occurrence of the crisis in the technology enabled Industries in India by adopting Risk assessing scale and Crisis prevention and intervention scale. The preliminary procedures in the exploratory research further helped the researcher in formulating the research problem and developing the objectives of the study.

Descriptive research is about describing what exists and may help to uncover new facts and meaning. This entails collecting data that would elaborate and provide detailed description of individuals, groups or situations under study. Instruments used to obtain data during descriptive studies include questionnaires, personal interviews and observation (checklists, etc.).

The method of data collection initially started with qualitative interviews of 10 Industry employees across various technology enabled organizations in India. This was important to understand the real outlook of the topic under study. The qualitative research interview is considered an idiographic approach which, as *Kvale* states, is trying to describe the world from the interviewee's point of view, unfold the meaning of people's experiences, and uncover their view of the world, before any scientific explanations are given. This approach was chosen in order to examine the topic, which evolve around situations that are highly complex, and as stated by many, are to some degree subjects of taboo. The interviews were semi-structured, and designed to only cover a limited portion of the topic. The framework chosen for the analysis, when applied on the collected data, assisted in creating an image of the different crises encountered across different companies, and of the causes, impacts, actions and lessons learnt from these. This overview was then used as base for preparing a final questionnaire.

In context of the present study, descriptive research proved helpful in examining the different constructs i.e. identification of prominent crisis in organizations of India, factors leading to occurrence of such crisis, identification of specific Crisis management models to combat occurrence of prominent crisis; and then understanding the concept of cybercrimes and its related problems prevalent in India.

The research methodology chosen to carry out the study can be divided into the following parts:

Part I: **Understanding the Research Problem:**

Theoretical Domains and Sub Domains: After having identified the main research issues, that are- Technological Crisis in industries of India, causes leading to such crisis; Crisis Management Models, an in depth study was conducted to understand their conceptual domains and sub domains.

Part II: **Literature Review and Identification of variables**:

Review of Literature: At this phase, an in depth review of literature was done to understand the researches that have been carried out pertaining to the study variables relating to prevalent crisis in Indian Organizations.

Variable Identification: An outcome of the review of literature was a set of most important variables that had been used through various research definitions and research papers; in order to define Crisis, Technological Crisis, factors leading to such crisis and Crisis Management models to combat such crisis.

Part III: **Development of Research Instrument**:

Development of Research Instrument: For development of a scale to identify a particular crisis in the Industry, a review of the construct, definitions and models of various Crisis was done. On the basis of intensity and frequency of occurrences of such crisis, the outcome was a set of factors that were tested through a pilot study using descriptive analysis and factor analysis.

Part IV: **Analysis of collected Data**:

The sampling technique used in the present study was “Purposive Sampling” The process of data collection was between January- June, 2020. The various tools and techniques used for analyzing the data for the study are also elaborated, in this section. This process was followed to preserve confidentiality and authenticity of responses. Moreover, respondents were pre informed about this process of data distribution and collection.

Table 1.10.1: List of Work of Selected Organizations

S. No.	Area of Work
01	Software Design and Development
02	Hardware Development
03	Information Technology Enabled Service (I.T.E.S)
04	Business Process Outsourcing (B.P.O)
05	Bank and Financial Institutions
06	Other Related Services

1.10.2 FORMAT OF MEASUREMENT:

There exist various formats for questions and it is generally considered good to decide the format of questions concurrently with the generation of items. This type of scale warrants that a statement is presented in declarative form with the help of response choices indicating different levels of agreement to the specified statement. It is expected that the difference of agreement should be approximately alike between any adjacent response options.

Survey Questionnaire contains overall 25 questions which covers the overall details of the respondents and main contention of this survey along with important questions relating to present cyber laws in India. The responses of main questions are objectives and coded as 1- Adequate and substantial, 2- should be enhanced, 3- Excessive and should be reduced and another set of questions are coded as 1- Yes and 2- No, the first set of 5 questions covers the personal information of respondent i.e., name, age and education etc.

1.10.3 PILOT TESTING:

Pilot test is done to measure the extent to which the instrument (questionnaire) is able to "provide data of sufficient quality and quantity to satisfy the objectives of the research". The main objective of pilot testing is to understand that the design of the questionnaire works in actual situation and to assess its reliability. To test the reliability and validity of the questionnaire, this questionnaire of initially pretested on *46* respondents of different organizations.

The draft of questionnaire used of pilot study contained the provision where respondents were invited to provide their suggestions in order to improve the quality of questions and questionnaire. Based on those suggestions, some of the questions were changed and edited, some more changes were made and the structure of the questions were improved.

1.10.4 QUESTIONNAIRE DESIGN:

The final questionnaire consisted of three parts.

The **Part I** covers the personal information of respondents and their professional or working details.

The **Part II** of the Questionnaire deals with the awareness related questions regarding the Information Technology Act, 2000 and the opinions of respondents on the of present cyber laws, India. Whether it is sufficient on curbing the problems relating to cybercrimes in India and provided them coded scale to objectify their opinion which provided diverse results due to different work sectors.

The **Part III** covers the questions relating to the opinion of respondents on the adequacy of compensatory amount and punishments related provisions of Information Technology Act, 2000 provided against the cybercrimes related to India. In order to analyze the opinions of respondents relating to the condition of present cyber laws in India. Moreover, the questionnaire asks respondent if they faced any form of cybercrimes during their working tenure.

In addition to this, informal discussions were also held with many of the respondents in order to get clearer insight of the topic and it was indeed helpful in carrying out the meaningful analyses. Published books, articles, magazines, journals, newspapers etc., were also referred to for the purpose of collecting the secondary data, in order to strengthen the theoretical or descriptive background of the study.

1.11. TENTATIVE CHAPTERIZATION/ RESEARCH DESIGN:

The research structure of this seminar paper is prepared on the basis of the scheme of chapterization enumerated as follows:

a) **Chapter 1**- *Introduction to the topic*- This chapter aims to cover and analyze the basic ideas relating to the crisis, technological crisis and crisis management with the perspective of Indian organizations, it also deals with the problem of cybercrimes in India and provides the broad perspective over the combined topic. It includes the brief background of the topic statement of problem, significance of study, aims and objectives of the study, scope and limitations of the study, research questions, important hypothesis, research methodology and overall design of the paper.

b) **Chapter 2**- *Crisis: Concepts, Theories and Jurisprudence*- This chapter tries to enumerate the detailed studies done by the several experts on the various concepts of crisis like types of crisis, consequences of crisis, technological crisis, anatomy of crisis, various responses towards crisis by Indian Organizations and analyses theories and other jurisprudence presented by the various experts relating to the crisis.

c) **Chapter 3**- *Organization Readiness*- This Chapter aims to evaluate the preparedness of Indian Organizations to face the multifarious challenges of crisis and the measures which can be taken by such organizations in order to efficiently deal with the problems of crisis in India. This paper analyses the position of such Indian Organizations.

d) **Chapter 4**- *Crisis Management*- This Chapter aims to provide various models provided by various experts relating to Crisis Management in dealing with various crisis faced by the Indian Organizations and this study tries to select best possible models as per Indian conditions.

e) **Chapter 5**- *Cyber Crimes in India: Meaning, Scope and Historical Aspects*- This Chapter aims to provide detailed explanations of the Concepts of Cybercrimes in India, by enumerating the meaning, describing the scope and tracing the Historical Aspects relating to the Cyber Crimes in India and describes the brief introduction of Cyber Crimes in India.

f) **Chapter 6**- *Jurisdiction for Cyber Crimes: Punishments and Preventions*- This Chapter tries to analyze the Jurisdiction for the Cyber Crimes in India and analyzes the provisions relating to the Punishments and Preventions relating to the crimes of cyber space in India and various aspects of studies relating to the problems of cybercrimes in India.

g) **Chapter 7**- *Indian Judicial Approach towards Cyber Crimes*- This Chapter aims to evaluate the Judicial prospects towards the Cybercrimes in India and deals with various pronouncements made by the Indian Judiciary towards the problems of Cybercrimes in India, especially faced by the Technology enabled organizations in India. This chapter also covers the opinions of eminent judges regarding this prevalent problem in India.

h) **Chapter 8**- *Comparative Study of Cyber Crimes*- This Chapter covers the critical comparative studies relating to the Cybercrimes in India along with the other countries in order to find the best suitable and reasonable measures for curbing this problem of cybercrimes and especially, covers that countries which can be idealized, who enacted the best suitable measures in their countries in order to find suitable measures which can be adopted in Indian conditions and find the best possible measures against such cybercrimes.

i) **Chapter 9**- *Critical Analyses of Data Collected*- This Chapter critically analyses the overall study relating to this topic by combining the technological crisis in the form of problems of cybercrimes face by the Indian organizations and Moreover evaluates the preparedness of such organizations in combating these problems of cybercrimes in India.

This study also analyses the sample collected relating to the penalties provision of cyber laws in India i.e., Information Technology Act, 2000. This study analyses the sample collected from various organizations in India and to study the cybercrimes faced by them, if any, in order to understand the type of attack faced by them for getting the best possible solutions in dealing with such cybercrimes faced by the organization in India.

j) **Chapter 10-** *Summary, Conclusion and Suggestions*- This Chapter finally enumerates this overall study which summarizes this comprehensive study along with the major findings. It also offers list of suggestions, both proactive and reactive in nature relating to this topic by providing the concluding remarks relating to this overall studies.

CHAPTER 2

CRISIS: CONCEPTS, THEORIES AND JURISPRUDENCE

> *"A real measure of a man is not where he stands at moments of comfort and convenience but where he stands at moments of challenge and controversy."*
>
> \- **Martin Luther King**

The word 'Crisis' is taken from the Greek word 'Krinein' which means 'to decide', "the turning point or the moment of decision or judgement", which can also be considered for "a sudden change for better or worse" or "a crucial of affair." As per Webster's, 1979 edition[46], a crisis can also be described as "a situation that has reached a critical phase". So, an unforeseeable time or state of affairs can be termed as crisis in which a huge change is impending. It can be either with a high possibility of an undesirable outcome, or with a highly desirable and positive outcome. A crisis is characterized by its degree of risk and certainty. Contrary to popular belief, a crisis not to be necessarily negative in nature but it may vary depending on the context for which it is being used. The term crisis can also be considered as a "acts of the gods" which increasingly becomes complex in its nature, trans-boundary and interconnected and considered as an unavoidable circumstance."

Technological crisis[47] in the organizations can be caused usually from the human application of science and technology in either negligent or erroneous manner and can also happen due to lack of sufficient knowledge to the applicant of such technology in the organization which may lead to such organization towards end. It may also cause when natural disaster disrupts in the normal daily routine during such application of technology. It may be easy for humans to heap about such technological breakdowns due to lack of human carefulness but usually not the same case when such crisis caused due to natural disasters.

[46] Dictionary by Merriam-Webster: America's most-trusted online dictionary, , https://www.merriam-webster.com/ (last visited Jul 23, 2020).

[47] Technological Crisis - BCMpedia. A Wiki Glossary for Business Continuity Management (BCM) and Disaster Recovery (DR)., , https://www.bcmpedia.org/wiki/Technological_Crisis (last visited Jul 23, 2020).

Technology based organizations are dynamic in nature. They acquire changes with the changing values, attitudes, visions and technologies due to changing times. The changing factors are dependent upon the people and upcoming innovations bought by them in the organizations through various factors in different ways. No matter how strong organization is or how fiercely it is developing, they all one thing common as an essential ingredient i.e., its Management.

Management is one of the key process of planning, organizing, conceptualizing, communicating and optimizing the resources of an organization in the pursuit to achieve specified organizational goals in efficient manner. Management is an important ingredient without which no organization could survive and develop.

One of the need of an hour for these organizations are managing the various crisis faced by them. As rightly quoted by **Geary W. Sikich**[48] that, Management is never put more strongly to test than in a crisis situation and pointed out by **Felix M. Lopez**[49], that 'A crisis indicates the period of instability, a stage in a sequence of events at which future events are determined. It is in the characteristics of a living organisms to face the crisis as it born, grows and finally dies. Human beings pass through it again and again and their journey from the beginning to old age; The way through which the crisis is met defines the eminent growth and steady decay of the individual controlling such organizations.

2.1. OPERATIONAL DEFINITIONS:

There are various authors and expert who tried defining the term 'crisis' and 'crisis management' by applying different lenses of situations through their own consensus in different ways which is not highlighted much in India by the researchers, among them some of the most suitable and important definitions are covered in the below-mentioned statements as:

2.1.1. CRISIS:

[48] Geary W. Sikich's research works, , RESEARCHGATE , https://www.researchgate.net/scientific-contributions/20759078_Geary_W_Sikich (last visited Jul 23, 2020).

[49] felix m. lopez – The World Journal, , https://huerfanoworldjournal.com/tag/felix-m-lopez/ (last visited Jul 23, 2020).

The **Webster Dictionary**[50], defined the term ‘crisis’ as, “turning point for better or worse’, as a ‘decisive moment’ or ‘crucial time’. It also defines the crisis as ‘a condition that has reached towards a critical phase”.

In the words of **Charles F. Hermann**[51], a crisis is “a situation that threatens the high priority goal of the organization for the purpose of its survival, which restricts the amount of time available for response and surprises the decision-makers through its occurrence, thereby endangering the high levels of stress in the organization”.

As per **Steven Fink**[52], “A crisis is an unstable time or a state of accident where a decisive change is impending- either one with higher possibility of an undesirable outcome or on the other side, higher possibility of extremely desirable or positive outcome, it generally has equal proposition to get the outcome on both the sides, but proper management can improve the odds”.

He further enumerated the crisis as, “a fluid, unstable, dynamic situation just like an illness and in a crisis, things are in a condition of constant flux”.

Pauchant and Mitroff[53] defined the term crisis in terms of disturbance to the whole system coupled with challenges to the basic assumptions of that system.

Rosenthlal U. & Pijenenberg[54], highlighted the broader concept of crisis in which, “the concept of crisis relates to situations featuring severe threats, uncertainty and the sense of urgency”.

[50] Dictionary by Merriam-Webster: America’s most-trusted online dictionary, *supra* note 46.

[51] James M. McCormick, *International Crises: A Note on Definition*, 31 THE WESTERN POLITICAL QUARTERLY 352–358 (1978), https://www.jstor.org/stable/447735 (last visited Jul 23, 2020).

[52] STEVEN FINK & AMERICAN MANAGEMENT ASSOCIATION, CRISIS MANAGEMENT: PLANNING FOR THE INEVITABLE (1986).

[53] Thierry C. Pauchant & Ian I. Mitroff, *Crisis management: Managing paradox in a chaotic world,* 38 TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE 117–134 (1990), http://www.sciencedirect.com/science/article/pii/004016259090034S (last visited Jul 23, 2020).

[54] Uriel Rosenthal Bert Pijnenburg, *Crisis Management And Decision Making: Simulation Oriented Scenarios* 2.

In the words of **Douglas G. Hearle**[55], “A crisis is a situation that, left unaddressed will jeopardize the organizations ability to carry forward business normally. The term is frequently used to address everything from a nagging issues to a hectic day”.

Laurence Barton[56], described the concept of crisis as, “A major unpredictable event that has potentially negative results. The occurrence and its aftermath may significantly damage an organization and its employees, services, financial conditions, products and goodwill”.

Clarke L. Caywood & Kurt P. Stocker[57], defined the term ‘crisis’ as, “immediately unexpected event or action that threatens the lives of stakeholders and ability of the organization to survive. While, various forms of crisis can be statistically expected (i.e., software breakdown or hardware failure), and its immediate happening is not, and results in crisis. The event which results in threat of life certainly be considered as crisis, when the lives of employees, clients, members of society and others who all are connected with the organization and stake in its action are threatened”.

In the book ‘Managing at the speed of change’, **Daryl R. Conner**[58] stated that, “A crisis is the point at which it becomes clear that what we had planned is no longer feasible and our expectations are disrupted. The disruption can be good or can be bad. But if it is a significant departure from what we expected, a crisis ensues because ambiguity enters the situation”.

In the works of **Michel Register and Judy Larkin**[59], they have consolidated the definition, mentioned below as:

“Crisis is an event which causes the company to become the subject of widespread, potentially unfavorable, attention from the international and national media and others such

[55] Douglas G. Hearle – Aug. 29, , PELHAM EXAMINER , https://pelhamexaminer.com/5070/obituaries/douglas-g-hearle-aug-29/ (last visited Jul 23, 2020).
[56] LAURENCE BARTON, CRISIS IN ORGANIZATIONS II (2 edition ed. 2000).
[57] THE HANDBOOK OF STRATEGIC PUBLIC RELATIONS & INTEGRATED COMMUNICATIONS, (Clarke L. Caywood ed., 1997).
[58] DARYL CONNER, MANAGING AT THE SPEED OF CHANGE: HOW RESILIENT MANAGERS SUCCEED AND PROSPER WHERE OTHERS FAIL (1993).
[59] Michael Regester & Judy Larkin, *Risk Issues and Crisis Management: A Casebook of Best Practice* (1998), /paper/Risk-Issues-and-Crisis-Management%3A-A-Casebook-of-Regester-Larkin/ced0e7fe4204f8ebca194042d110a222eaba2f01 (last visited Jul 23, 2020).

as clients, customers, shareholders, employees and their families, politicians and environmental pressure groups who all, for one reason or the another, vested the interest in the activities of the organization".

2.1.2. TECHNOLOGICAL CRISIS:

Before proceeding towards the definition of technological crisis, it is pertinent to cover the few definitions of technology as well, which all are covered below:

According to the **Merriam-Webster Dictionary**[60], technology is defined as:

1. The practical application of knowledge especially in a particular area; (b): a capability given by the practical application of knowledge.
2. A manner of accomplishing a task especially using technical processes, methods, or knowledge.
3. The specialized aspects of a particular field of endeavor.

According to the **Oxford Dictionary**[61], the term technology is defined as:

1. The application of scientific knowledge for practical purposes, especially in industry.
2. Machinery and devices developed from scientific knowledge.
3. The branch of knowledge dealing with engineering or applied sciences.

Emmanuel G. Mesthene's[62] terrific little 1970 book, *Technological Change: Its Impact on Man and Society* defined the term 'technology' as:

"The technology is the organization of knowledge for the achievement of practical purposes."

[60] Dictionary by Merriam-Webster: America's most-trusted online dictionary, *supra* note 46.

[61] Home : Oxford English Dictionary, , https://www.oed.com/ (last visited Jul 23, 2020).

[62] J.A. Raffaele, *EMMANUEL G. MESTHENE. Technological Change: Its Impact on Man and Society. Pp. 127. Cambridge, Mass.: Harvard University Press, 1970. $4.95*, 393 THE ANNALS OF THE AMERICAN ACADEMY OF POLITICAL AND SOCIAL SCIENCE 181–182 (1971), https://doi.org/10.1177/000271627139300166 (last visited Jul 23, 2020).

The profound author **W. Brian Arthur**[63], in his book *The Nature of Technology: What It Is and How It Evolves,* provided the three major conception regarding the term technology as:

1. "The first and most basic one is a technology is a means to fulfill a human purpose. … As a means, a technology may be a method or process or device… Or it may be complicated… Or it may be material… Or it may be nonmaterial. Whichever it is, it is always a means to carry out a human purpose.
2. The technology is an *assemblage of practices and components*."
3. the entire collection of devices and engineering practices available to a culture."

Historian **Robert Friedel**[64], in his 2007 book, *'A Culture of Improvement: Technology and the Western Millennium'*, University of Maryland, he offers a formal definition of technology to kick off the book and then ends with a less formal one:

"By technology we typically mean the knowledge and instruments that humans use to accomplish the purposes of life."

At the end, he finally noted that

"Technology can, indeed, be defined as a pursuit of power over nature."

The above mentioned statements covered the broader ambit while enumerating the concept of technology.

According to **BCM Institute**[65], "Technological crisis arises when the humans applies any science and technology and certain breakdown arises which are the results of the failure in application of such technology. The problem may also arise due to disruption in the overall system which finally leads to the crisis. Breakdown of machine, corrupted software are the famous examples of technological crisis. This generally occurs when the

[63] W. BRIAN ARTHUR, THE NATURE OF TECHNOLOGY: WHAT IT IS AND HOW IT EVOLVES (Reprint edition ed. 2011).

[64] A Culture of Improvement: Technology and the Western Millennium by Robert Friedel, RESEARCHGATE ,https://www.researchgate.net/publication/42972842_A_Culture_of_Improvement_Technology_and_the_Western_Millennium_by_Robert_Friedel (last visited Jul 23, 2020).

[65] BCM Institute - Homepage, , BCM INSTITUTE , https://www.bcm-institute.org/ (last visited Jul 23, 2020).

technology being applied by the organization or the individual is complex in nature and which leads to system breakdown".

As rightly quoted by **O. Lerbinger**[66], in his work '*The crisis manager: Facing Risk and Responsibility*' that "Technological Crisis are caused by the human application of science and technology. Technological mishaps inevitably occur when technology becomes complex and coupled and something goes wrong in the system as a whole (technological breakdowns). Some technological breakdowns occur when human error causes disruptions (Human breakdowns). People tend to assign blame for a technological disaster because technology is subject to human manipulation whereas, they do not hold anyone responsible for natural disaster. When an accident creates significant environmental damage, the crisis is also categorized as mega-damage."

According to **Clint Fontanella**[67], highlighting the concept of technological crisis is very crucial for the today's technology based organizations, for which, he emphasized on the reliance of today's organizations on the technology for the performance of its day to day function. So, when the Ecommerce sites and software companies can lose millions of potential leads if their servers suddenly break. That's not only a huge loss of potential revenue, but it's also a major hit to the product or service's reputation.

2.1.3. CRISIS MANAGEMENT:

Various authors and researchers tried defining the term 'Crisis Management' in different manner as:

According to **Micheal Register (1990)**[68], "the crisis management is about seizing the initiative, taking control of what has happened before it engulfs the company".

[66] Lerbinger O 1997 The crisis manager Facing risk and responsibility Mahwah NJ | Course Hero, , https://www.coursehero.com/file/p52an47g/Lerbinger-O-1997-The-crisis-manager-Facing-risk-and-responsibility-Mahwah-NJ/ (last visited Jul 23, 2020).

[67] Clint Fontanella, *How to Create a Social Media Crisis Management Plan [Free Template]*, https://blog.hubspot.com/service/social-media-crisis-management (last visited Jul 23, 2020).

[68] Risk Issues and Crisis Management : Michael Regester : 9780749443825, , https://www.bookdepository.com/Risk-Issues-Crisis-Management-Michael-Regester/9780749443825 (last visited Jul 23, 2020).

As per **Steven Fink**[69], described “crisis management as the art of removing much of the risk and uncertainty to allow you to achieve more control over your own destiny”.

According to **Robert**[70], crisis management may be defined as the “taking decisions or finding solutions for crisis situations”.

Whereas **Pearson and Claire**[71], defined the term Organization Crisis Management as “a systematic attempt by organizational members with external stakeholders to avert crisis or to effectively manage those that do occur” They also stated that, “organizational crisis management process effectiveness is the evidenced when the potential crisis are averted or when the major stakeholders affirms that the success outcome of short and long range impact of crisis outweigh the failure outcomes”.

According to **Goel (2009)**[72], Crisis management consists of:

1. Methods used to respond to both the reality and perception of crises.
2. Establishing metrics to define what scenarios constitute a crisis and should consequently trigger the necessary response mechanisms.
3. Communication that occurs within the response phase of emergency management scenarios.

The real issue is not just to recognize the crises, but to address them in a short time and with a will to address the issues they represent like the early warning signs and its system or software and the possibility of a future national crisis, to bring the complex factors into focus in such a manner that individuals can understand and marshal the forces necessary to address the situation.

Finally, in present times, the definition given by **Laurence Barton**[73], would be considered as nearly appropriate, which being repeated as “crisis is a major unpredictable

[69] FINK AND ASSOCIATION, *supra* note 52.

[70] Bertrand Robert & Chris Lajtha, *A New Approach to Crisis Management*, 10 JOURNAL OF CONTINGENCIES AND CRISIS MANAGEMENT 181–191 (2002), https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-5973.00195 (last visited Jul 23, 2020).

[71] Christine M. Pearson & Judith A. Clair, *Reframing Crisis Management*, 23 THE ACADEMY OF MANAGEMENT REVIEW 59–76 (1998), https://www.jstor.org/stable/259099 (last visited Jul 23, 2020).

[72] MAJOR SURESH GOEL, CRISIS MANAGEMENT: MASTER THE SKILLS TO PREVENT DISASTERS (2009).

[73] BARTON, *supra* note 56.

event that has potentially negative results. The occurrence and its aftermath may significantly damage an organization and its employees, services, financial conditions, products and goodwill".

2.2. CASES OF TECHNOLOGICAL CRISIS:

Crisis can be faced by any of the organisation. The literature divides crisis primarily into two units i.e., natural and man-made crises. Firstly, Natural crisis are catastrophic in nature which resulting from natural influences such as volcanic eruptions, tornadoes, earthquakes, etc., over which man/human has no control. Whereas, Man-made crisis, on the other hand, are those catastrophic causes that results from human choices and decisions. What defines a crisis in business operations depends on a number of variables such as: the nature and scope of the event; importance of the issue towards the stakeholders involved impact on other firms and industries; how many and how quickly individuals inside and/or outside of a particular firm need to be helped or informed; who and how many people need interpretation of the events, and how accessible those individuals are; how much communication with the media is required; what the media choose to focus on; who and how many people need emergency care; how much the organizations needs to take the control and demonstrate that it is capable of responding; and how quickly the firm needs to respond.

The famous cases of crisis faced by Indian organizations, especially on cyber space, is the Cyberattack happened on **Cosmos Bank**[74], in the year 2018, where the Pune based bank faced a huge loss of almost 94 Crore Rupees through the Malware Attack on the switching system which was one of the first case where the communication between Payment Gateway and bank was breached due to lack of proper management towards such crisis. Another famous case is attack on **Canara Bank's**[75] ATM Servers which resulted in a loss of almost 20 lakh rupees from various bank accounts. This event victimized more than 50 clients and exposed the bank account details of more than 300 clients across India. The reason behind such mishap was misuse of confidential data, which obviously caused

[74] Cosmos Bank – Cosmos Bank, , https://www.cosmosbank.com/ (last visited Jul 23, 2020).

[75] Canara Bank, , https://www.canarabank.com/ (last visited Jul 23, 2020).

due to lack of security measures and management problems by the organizations end which again can be dealt with the problem management process beforehand.

As per the data shared by the **Indian Computer Emergency Response Team**[76] between the year 2017 & 2018, the total number of cases of website hacking was ranged at 22,000 and among them 114 websites were officially created and operated by the wings of government. The main reason behind such negative operations is to gather the details of as much clients as possible in their network and to shatter their reputation in best possible manner. Again this event could have also been avoided if the organizations would have themselves well-prepared before happening of such attacks through improving their crisis management process both internally and externally.

Another famous example is the phishing attack on the famous brand company of India **Wipro**[77], the news portal of the company was attacked through the trap of gift card. The case of example of failure in the management of personal data employees as well clients which could have been avoided. Other famous case is of **Justdial**[78], which resulted in the expose of personal data of various clients due to unprotected API security which caused this incident which another case which needs to be looked serious concern for their management process.

Another famous case which shadowed various times in the news but failed to be authenticated was the case of data leakage of **Aadhar**[79], which may be proved, could be categorized as biggest case of mismanagement by any government agency i.e., **UIDAI**[80] of India which was although not authenticated but claimed by many sources to be true but all those allegations were negated by the government.

[76] Indian - Computer Emergency Response Team, , https://www.cert-in.org.in/ (last visited Jul 23, 2020).

[77] Wipro | Digital, Technology, Business Solutions, , https://www.wipro.com/en-IN/ (last visited Jul 23, 2020).

[78] Justdial - Local Search, Social, News, Videos, Shopping, , https://www.justdial.com/ (last visited Jul 23, 2020).

[79] Get Aadhaar - Unique Identification Authority of India | Government of India, , https://uidai.gov.in/my-aadhaar/get-aadhaar.html (last visited Jul 23, 2020).

[80] Unique Identification Authority of India, , UNIQUE IDENTIFICATION AUTHORITY OF INDIA | GOVERNMENT OF INDIA , https://uidai.gov.in/about-uidai/unique-identification-authority-of-india.html (last visited Jul 23, 2020).

This is high time where government agencies should look forward towards such form of technological crisis emerging in India at enormous rate which can be curbed through appropriate management process which needs to be equipped by various Indian organizations in order to deal with such menace in the most effective and efficient manner and make themselves advancing with the changing time across the world to set positive example.

Whereas, some other most popular crisis examples that are known to the world and which became case studies for researchers are the popular "*product tampering*" case of **Johnson and Johnson Tylenol Crisis**[81] and **Pepsi syringes crisis**[82] case. These crises have been hailed as one of the well-handled organization crisis in history because of the fact that the company acted responsibly and acted fast. **Nestle's**[83] two-minute noodles brand **Maggi**[84] which became a face of internal crisis recently in India becoming renowned also because of their process through which such brand has bounced back by strongly gaining 57 % market shares can also be considered as one of the finest example of "Crisis well managed".

Some of the other famous examples of Indian Crises is the accident at Bhopal, India also known as Bhopal Gas Tragedy is one of the famous example of crisis. The high magnitude of this tragedy stunned all the countries in the world and was also commented by the FORTUNE magazine titling it as "Crisis badly managed". Exxon Valdez Oil Spill's[85] accident Crisis is also one of such example of ineffective crisis management which needs to be highlighted. Not much famous but more acute in nature, however, is that crisis

[81] http://daisywheelinteractive.com, *Johnson & Johnson and Tylenol - Crisis Management Case Study*, MALLEN BAKER - CHANGE IS A LEARNABLE PROCESS (2008), http://mallenbaker.net/article/clear-reflection/johnson-johnson-and-tylenol-crisis-management-case-study (last visited Jul 23, 2020).

[82] Pepsi's Crisis Response: The Syringe Scare: PRSA, , https://apps.prsa.org/SearchResults/view/6BW-9412B04/0/Pepsi_s_Crisis_Response_The_Syringe_Scare (last visited Jul 23, 2020).

[83] NESTLÉ , https://www.nestle.in/home (last visited Jul 23, 2020).

[84] William Comcowich, *PR Crisis Management Lessons from the Nestlé Maggi Noodle Controversy*, GLEAN.INFO (2018), https://glean.info/pr-crisis-management-lessons-from-the-nestle-maggi-noodle-controversy/ (last visited Jul 23, 2020).

[85] *Exxon Valdez* oil spill, , WIKIPEDIA (2020), https://en.wikipedia.org/w/index.php?title=Exxon_Valdez_oil_spill&oldid=968001145 (last visited Jul 23, 2020).

which has affected the smaller industries in the unorganized sector — the sector that employs almost 80% of all manufacturing workers in the country.

After various years of keeping their working process safe and appointing internally-bright candidates as the CEOs, India's billion-dollar organizations are waking up to a new world of practical possibilities and increasingly picking the outsiders for the high level job, a trend that always possibly reflects a deeper internal crisis in the Indian organizations. But, the current looming technological crisis across various technology based sectors is an alarming time for the leaders to strategize their moves in controlling the rising attrition rate in order to prepare the organization for all the future chances of such crisis and make the core team aware and well-prepared about any of such crisis in order to efficiently deal with them.

India has already been plagued by different types of crisis on both organizational as well as at international front since decades. So, it is crucial for such organizations identifying the different forms of crisis and preparing strategies to control them which can be the only way to minimize the technological i.e., human and financial which ultimately leads to the reputational loss stirring out of it of such organization.

Following the definition of Crisis[86], the crisis is often not accidental; the symptoms of the possibility of its occurrence can be sensed and observed. Therefore, organizations that generally become ignorant and fail to cope and deal with human resources issues will land up in crises, such as job dissatisfaction among employees, reduced commitment, lower work quality, poor morale, burn out, poor judgments and which ultimately make them a host of unhealthy consequences which leads to crises. Though, such elements are very common among the employees across all the organizations, the impact of such is large as it adds to stress in employees, which can also affect their job performance, mental well-being, and physical health too. Such technological crises also lead to negative perspective

[86] Burkiewicz, Ł., Knap-Stefaniuk, A. (2020). Modern Managers and Cultural Diversity In The Workplace. IN: Education Excellence and Innovation Management: A 2025 Vision to Sustain Economic Development during Global Challenges. The 35th IBIMA Conference on 1-2 April, 2020 Seville, Spain. 7474-7483., , RESEARCHGATE , https://www.researchgate.net/publication/342903036_Burkiewicz_L_Knap-Stefaniuk_A_2020_Modern_Managers_and_Cultural_Diversity_In_The_Workplace_IN_Education_Excellence_and_Innovation_Management_A_2025_Vision_to_Sustain_Economic_Development_during_Global (last visited Jul 23, 2020).

about work among employees. Ultimately, this negative outlook towards work often spreads towards their co-workers and can also have a cynical impact on everyone's performance.

2.3. IMPORTANCE OF TECHNOLOGY BASED PROFESSIONALS:

Mostly, in the technology based organizations, the Hardware or Software professionals are those sensitive gatherings of employees who contribute significantly towards the financial achievement of the organizations through their knowledge, expertise and work efficiency. This is based on the analogy that today's greater extent of work content requires new and trending learning creation and which leads to the development of human capital, which reflects the quality yield of their thoughts and productivities and demonstrates that the climb of learning work makes such technology equipped employees more profitable and appealing towards the organization than their requirement towards the organization. The significance of such professionals and their technical insights is being positively perceived by the new economy of the country. This is on the account of their technical insight which is the main resource of the organization and which can't be easily and effectively reproduced by any other, and is a wellspring of profit, expertise and feasible upper hand.

Through the changing era, dispersal, application, and reuse of unsaid learning, organizations can put forward creative thoughts for persistent new item improvement and in this manner maintain an upper hand. So, such professionals are seen as resources for the organizations which should be produced and developed, though manual specialists are seen as an expense to organizations which should be controlled and decreased. All in all, product development professionals have a high level of skill, training, or encounter, and the basic role of their employments includes the creation, dissemination, application and reuse of information.

Recently, the Ministry of Electronics & Information Technology (MeitY)[87] in partnership with Atal Innovation Mission - Niti Aayog[88] has launched Digital India Atma

[87] Ministry of Electronics and Information Technology, Government of India | Home Page, , https://www.meity.gov.in/ (last visited Jul 23, 2020).
[88] Atal Innovation Mission | NITI Aayog, , https://niti.gov.in/aim (last visited Jul 23, 2020).

Nirbhar Bharat App Innovation Challenge for Indian tech entrepreneurs and start-ups. This shows that cooperation and correspondence are likewise fundamental parts of the profitability of such professionals. In the past, studies of researchers have been focused on that the future economy is about information and connections, since interpersonal organizations can empower individuals to investigate thoughts, grow new ideas and learn in the ways that will be progressive. Furthermore, the accomplishment of a business is esteemed to depend on the powerful administration of technology based workers, in which such administrators can inspire them to share their area information by providing them self-governance of occupation outline.

2.4. FACTORS LEADING TO TECHNOLOGICAL CRISIS:

Major Events in industries such as **Bhopal**[89] disaster in India in 1984, **Sozo**[90] accident in Italy in 1975 and the famous **Psovdnia**[91] accident in Texas in the US in 1989 to wide variations in patterns of process safety, deal with emergency situations and crisis management were derived. These accidents may be caused by process failures, defective design, defective equipment, human error or external factors such as floods, earthquakes and terrorism is a bad thing. Accident statistics suggest that the crisis management process is an important problem in the process industry and to think of ways to control and eliminate the hazards and achieve a level of reliability.

On the other hand, short overview of some of these points are indicative of the last twenty years, since the crisis, many oil and gas industry have occurred in the downstream sector, most similar to the maligned, or even have a predictable and delays caused by employees or managers have occurred. In other words, the components of which are predictable.

Table 2.4.1. Factors leading to Crises faced by Organizations in India:

Technological	Financial	Marketing	Others

[89] Bhopal disaster, , WIKIPEDIA (2020), https://en.wikipedia.org/w/index.php?title=Bhopal_disaster&oldid=967071886 (last visited Jul 23, 2020).
[90] Ali Reza Nojoumi, Saeid Givehchi & Amir MahmoodZadeh, *Crisis Management Arising from Technological Risks and its Models in South Pars: A Systematic Review* 10 (2015).
[91] *Ibid.*

Machinery Breakdown	Capital Problem	Demand Shortage	Ineffective government regulations
Software failures/hacked	Expensive Construction Costs	Heavy competition	Negative news by Media
Low quality Hardware	Reduction in turnover	Inadequate Pricing Policies	Sudden death or resignation
Problem of Power supply	Siphoning off money	Tampering with Products	Natural Disaster

All the above mentioned factors affects the organizations in India adversely and it is observed that the technological crisis is getting more prominent in the recent times which affects the quality of the working process of the organization which leads to heavy loss and shut down of such organization.

One of the major reason behind this technological crisis in India is firstly, the lack of honesty over the human resources i.e., the management level staff in approving for the buying of low-quality products as many of them are satisfied with the alternates which are of cheap price and easily available and can be compromised with the high-quality products. Moreover, which is also supported by the leaders which becomes unfortunate practice by the organizations which in long term leads to negative outcome to such organization and results in technological crisis.

Most of the technology based professionals are not aware about the laws relating to the technologies in India and such lack of knowledge about the legal remedies make even more sensitive feelings to move towards the law for acquiring appropriate legal remedies which also closes one door to lead management process through the awareness of legal remedy against any crisis caused to intentional wrongful activity caused by any employee of the organization.

It is pertinent to note that the inferences[92] in critically figuring out the causes of crises which can also be observed as per conditions of Indian organizations are:

1. Problems of crisis build up over the time. There are many contributory factors for the incident although very few among them needs to be emphasized over others.
2. The method of execution is often the main cause of crises.
3. Frequent change of working environment also leads to the crisis.
4. Proper chance factor also causes crisis.
5. The main reason behind any crises is due to fault in the interpretation of organizational management or weak organizational concepts like decentralization, diversification or control or due to the excessive or inadequate implementations or failure in making compensatory actions, such as a more sophisticated information and control system for the chain of senior management following structural decentralization.
6. Crisis may often lead to the positive or beneficial effects by forcing the taking of long overdue action.
7. Crisis could be strategically avoided by keeping the organization competitive, reaching out for the opportunities without going overboard, proper supervision of the chief executive by the board of directors and towards the organization by the chief executives, the ability to distinguish between real trouble from the normal operating difficulties, and by management having the courage to face up to the real trouble in time.

Table 2.4.2. Four Stages of Crisis Development:

Crisis Denial

↓

Hidden Crisis

↓

[92] Crisis and Aftermath: Community Psychiatry in Saskatchewan, 1963-69* - Colin M. Smith, 1971, , https://journals.sagepub.com/doi/10.1177/070674377101600110 (last visited Jul 23, 2020).

Organization Disfiguration

↓

Collapse of Organization

↓ ↓

Recovery Failure

Source: Stuart Slatter and David Lovett (1999), *'Corporate Turnaround, Managing companies in distress'*, London, Penguin Books.[93]

Among all the above mentioned stages, it is crucial to highlight the initial stage i.e., hidden crisis stage, the management team and organization is generally ignorant or unaware about the existence of a crisis. Mostly, this is due to the inadequate process control system- not just specific segment system, but also other informal systems in order to monitor and interpret the unexpected contingent events. There are cases in India where, certain organizations become complacent and overconfident about their capabilities and position in their sector. Once the sign of crisis become visible in the organization (second stage), managements starts looking for reasons behind such crises and tries to make it away. At this juncture, two contentions can be put forward, firstly, the signs of crises become visible due to organizational efforts to change and due to the hard work done for the purpose of improving its performance. Secondly, due to the poor performance of organization caused due to various reasons but mainly due to the short-term environmental pressure which is beyond the control of organization itself. It is important to note that, both the contentions lead towards one common point that the management action is not a only or necessary step to avert the crises. As there are chances when organization faced the lethal crisis have been likened to places perched to mountain top that were crumbing from erosion.

At the third stage of the crisis development, management group finally recognizes the presence of crisis and start taking preventive steps but the need of the required action

[93] Corporate Turnaround (Penguin Business): Slatter, Stuart St. P., Lovett, David: 9780140279122: Amazon.com: Books, , https://www.amazon.com/Corporate-Turnaround-Penguin-Business-Slatter/dp/0140279121 (last visited Jul 23, 2020).

is always underestimated. The decision making team eventually become smaller as the autocracy enters the room in order to maintain secrecy and improved coordination in order to face such challenges effectively. But at the same time with less consultation and shortage of time, there are greater tendency to rely on those who have full faith and wisdom towards the organization. The actions which can be taken at the third stage have the potential to temporarily slow-down the damage and help to sail through from the problems of crisis faced by the organization.

At the fourth stage, the organizational cracks eventually result in collapse. This incident makes it evident to everyone that sometimes even top level management teams also make faulty speculations and results in crisis which creates severe doubts as to whether such managements are capable in coping up with the crises.

2.5. RIPPLE EFFECT OF A CRISIS:

The capacity of a crisis to cause the other crisis situation is popularly known as the ripple effect of crises because these crisis spreads out like ripple just like after the stone is thrown into the pool of water. The first initiated crises play the role of stone striking in the water i.e., organization. The subsequent impact which become the major reason behind the damage may include the stone striking at the very bottom of the pool, the impact of such strike result in the splashes of water on the pool surface and surrounds and the damage caused by the ripples on the pool shore lines. The ripple effect is the subsequent reaction to the previous crisis that may be caused due to the poor performance of the technical management group towards such original crisis situations.

Such crisis situation caused may result in different ripple effects in various organizations and groups. For instance, the technology based organization that is destroyed due to huge technological damaged assets drains large money from the organization, puts people out of work and may possess potential to cause further damage to the near related community system through the loss of required resources. Sometimes, these ripple effects may cause such form of damage which is even larger loss than that of initiating crises, for example, a software based company may be destroyed due to damage in the hardware of requires system which is such massive in nature result in closedown of the service oriented company.

2.6. ANATOMY OF A CRISIS:

Fink[94] has already studied about the various stages involved in disseminating the crisis. According to him, the stages of crisis can consist of as many as mainly four different and distinct phases. Since, the crisis can also be viewed as a highly critical disease, he named all the four stages as: prodromal crisis stage, acute crisis stage, chronic crisis stage and the crisis resolution stage.

The first stage, **Prodromal crisis stage**[95], is considered to be the foremost warning stage and also denoted as the pre-crisis stage. In case of the adverse turning point, when the case of prodrome in the organization, is entirely missed, then the acute crisis may strike next. The **Acute crisis stage**[96], is the time from where there is no return. It is the stage at which at least some amount of damage has been done. Whether there will be some additional damage or not is to be totally based on the way of handling of this stage by the organization. According to the researcher, it is mostly acute crisis stage which people have in mind when they speak about the crisis faced by them. The next stage is the **chronic crisis stage**[97], which is also known as the clean-up stage or the post mortem. This is the also considered as the period of recovery through the process of self-analysis, of self-doubts and of healing. Skillful employee will use it very wisely as a good time for the future crisis management planning, analyzing what actually went right or actually what went wrong and taking appropriate actions. The **Crisis resolution stage**[98], is the fourth and

[94] FINK AND ASSOCIATION, *supra* note 52.

[95] The Four Stages Of A Crisis Management Essay, , https://www.ukessays.com/essays/management/the-four-stages-of-a-crisis-management-essay.php (last visited Jul 23, 2020).

[96] The Three Stages Of A Crisis, , https://blog.pocketstop.com/the-three-stages-of-a-crisis-8585 (last visited Jul 23, 2020).

[97] Katsuyuki Kamei, *Crisis Management*, *in* SCIENCE OF SOCIETAL SAFETY: LIVING AT TIMES OF RISKS AND DISASTERS 141–150 (Seiji Abe, Mamoru Ozawa, & Yoshiaki Kawata eds., 2019), https://doi.org/10.1007/978-981-13-2775-9_13 (last visited Jul 23, 2020).

[98] The Brain, *The Stages of Crisis: Understanding the crisis management lifecycle*, https://www.noggin.io/blog/the-stages-of-crisis-understanding-the-crisis-management-lifecycle (last visited Jul 23, 2020).

the final stage that should be the crisis management goal during the preceding three phases. It is actually at this stage that all efforts are taken to turn the crisis into an opportunity.

2.7. CONSEQUENCES OF CRISIS:

Any crises may result in a relative degree of success or failure. It is also evident that no organization can be completely prepared to be effective in all the aspects of any crisis.

The below mentioned **Table 2.7.1.** provides the various forms of cause and consequences of a crisis as listed below as follows:

Table 2.7.1. Successes and Failures of Crisis Management Models[99]

Crisis Concern	Failure outcomes	Mid-ground outcomes	Success
Signal Detection	Ignored and caught unaware	Becomes alert	Detected early and appropriate response
Incident containment	Beyond boundaries of organization	Slight damage to those beyond organization boundary	Impact contained within and no stakeholder injury.
Business Resumption	Operation shutdown downtime is lost	Affected operation closed temporarily Downtime minimum	Business as usual no loss of product or service delivery
Effects on learnings	No learning similar crises recur	Learning occurs	Changes in policies and procedure, lessons applied to future incidents

[99] Pearson and Clair, *supra* note 71.

Effects on reputation	Negative repercussions, Public perceives organization as a villain	Negative effect short-lived Public perceives errors as minor	Image improves, public perceives organization as caring
Resource availability	Lacks essential	Scrapes by on own and ad hoc assistance	Own and external resources available for response
Decision-making	Slow and fancy driven	Slow, due to extra organizational constraints	Timely decision and based on facts

2.8. CASE STUDIES AND CONCEPTUAL APPROACHES:

Nearly, 90 % of corporations in India store their informations in the digital form which also includes internet based electronic commerce, online banking and stock trading, corporate usage information and storage of official mails, phone messages and electronic logs. The risks associated with this information are many. There have various cases relating to such crisis in organizations. According to a new Data Security Council of India (DSCI)[100] report, India is being the second most affected country who faced cyber-attacks due to which many organizations in India looking for the optimum cyber insurance policies in order to manage such crisis effectively. As, according to the data of CISCO Annual Cyber Security Report[101], almost 53% of all cyber-attacks resulted to financial damages of even more than $500K (including lost revenue, opportunities, and various out-of-pocket costs among others) for the organizations alone in the year 2018-19.[102]

In the Indian context, when it comes to the data theft and data breach, the first recent case which comes in mind is **Aadhar[103]** case. In February 2019, personal details of Aadhar

[100] Data Security Council of India (DSCI), , https://www.dsci.in/ (last visited Jul 23, 2020).

[101] Cybersecurity Reports, CISCO, https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html (last visited Jul 23, 2020).

[102] *Ibid.*

[103] Aadhaar - Unique Identification Authority of India | Government of India, *supra* note 34.

of over 6.7 Million users containing details such as the names, address and contact number were got leaked on Indane's website[104]. Also, Prior to this in the year 2018, French cybersecurity expert Baptiste Robert (who is also known by another pseudonym as Elliot Alderson on Twitter) had uploaded website links containing the Aadhaar data of thousands of Indian citizens. And that's just two examples among multiple leaks related to Aadhaar from the state government bodies. Other Indian startups including Pune-based fintech company **EarlySalary**[105], restaurant discovery company **Zomato**[106], foodtech startup **FreshMenu**[107] and travel platform **Ixigo**[108] have also witnessed data breach cases. Another famous case which came up in front in the year 2019, cyber-attack on the Indian based Healthcare websites, as claimed by the US based cyber security firms. The system breaker stole almost 68 lakh records of patients as well as doctors.

Furthermore, there is one important case known as '**SIM Swap Scam**'[109], it was case of cyber-theft of nearly four crore rupees from several bank accounts, the operation of illegal transferring of money from various bank accounts of several individuals. The operation was made by gaining SIM card information through wrongful means and through the fake documents, the criminals carried out the transactions through the process of online banking. But later, such criminals were finally got arrested but set an example for the preparedness in future.

It is also essential to note one more case of cyber-attack on the Pune based regional bank i.e., **Cosmos Cooperative Bank Ltd.**[110], this incident shook whole banking sector of India when hacker transferred almost 94.42 Crore Rupees. The stealing was done by hacking the servers of ATM and took details of various Visa and Rupay debit cardholders. Hackers wiped out money and transferred it to a Hong Kong situated bank by hacking the server of Cosmos Bank. A case was filed by Cosmos bank with Pune cyber cell for this

[104] Indane Online : Online Gas Booking and Services, , https://indane.co.in/ (last visited Jul 23, 2020).
[105] EarlySalary, WWW.EARLYSALARY.COM , https://www.earlysalary.com (last visited Jul 23, 2020).
[106] Zomato India, , https://www.zomato.com/ncr (last visited Jul 23, 2020).
[107] FRESHMENU , https://freshmenu.com (last visited Jul 23, 2020).
[108] ixigo - Flights, Train Reservation, Hotels, Air Tickets, Bus Booking, , https://www.ixigo.com (last visited Jul 23, 2020).
[109] SIM swap scam, , WIKIPEDIA (2020), https://en.wikipedia.org/w/index.php?title=SIM_swap_scam&oldid=965932687 (last visited Jul 23, 2020).
[110] Cosmos Bank – Cosmos Bank, *supra* note 74.

cyberattack. The switching system acts as an interacting module between the payment gateways and the bank's centralized banking solution was attacked. The attack was the Malware attack on the switching system raised numerous wrong messages confirming various demands of payment of visa and rupee debit card internationally. The total transactions were 14,000 in numbers with over 450 cards across 28 countries. At the national level, the amount was taken through 400 cards and the transactions involved were 2,800. This was in fact the first malware attack in India against the switching system of bank which broke the communication between the payment gateway and the bank. It is the finest example in front of banking organizations to verify the potential vulnerabilities which can be fished out and in order to make the entire digital part of the banking system safe.

Another one is the case of hacking in Canara Bank ATM Servers[111], the hackers wiped off almost twenty lakh rupees from various bank accounts. The number of victims was nearly 50 and it was traced that hackers were holding the account details of more than 300 ATM users across India.

Another case is of **Amitabh Bachchan**'s[112] twitter handle which was also got hacked and the perpetrators posted hateful messages and communal message which shocked almost everyone. They set the example for the big companies also. However, if the news gets out this can be a huge blow to the credibility of any company.

2.9. CRISIS AND CHANGE:

Stuart Slatter and David Lovett (1999)[113], have studied the relationship between crisis and change. According to their research, once crisis becomes severe and both management in the form of individuals and the organizations as a whole have begun to show some of the negative behavioral characteristics, drastic level of action is needed if optimum level of recovery is to be achieved. If the onset of crisis is traced early enough by

[111] Is your money safe? Bank ATM fraud cost these people Rs 9 lakh; this is how | Zee Business, , https://www.zeebiz.com/personal-finance/news-is-your-money-safe-bank-atm-fraud-cost-these-people-rs-9-lakh-this-is-how-57984 (last visited Jul 23, 2020).

[112] Amitabh Bachchan (@SrBachchan) / Twitter, , TWITTER , https://twitter.com/srbachchan (last visited Jul 23, 2020).

[113] Corporate Turnaround (Penguin Business): Slatter, Stuart St. P., Lovett, David: 9780140279122: Amazon.com: Books, *supra* note 93.

the organizations, a serious crisis may be averted and less volatile action may be necessary to proceed.

They have critically pointed out that, the earlier the developing crisis is traced and tackled, the less changes will be necessary in the organization and the more chances that there is of saving the firm and instituting the successful turnaround by the organizations.

As per the observation made through the detailed explanation of the concepts of crisis, it may be observed that it may be proved as the high level of danger towards the organization’s health and may lead towards its collapse.

Therefore, this topic highlighted the meanings, definitions, concepts, patterns and ideologies relating to crises in order to put some light on the losses it may cause and how easily it may take down even the strongest firms or organizations on their feet if left unnoticed or delay in noticing it. But such problems can be contained if the right approaches to be implemented effectively at the right moment. The technical and management teams along with leaders play very important role for the purpose of tracing the crisis and in order to apply the right approaches towards it to control it at right time and stopping it from getting even worse and to understand the methods which may be suitable for the technology based organizations while dealing with any sort of perils or any big crises.

The upcoming chapter tries to cover the ideas, methods, factors, guidelines and approaches used by the organizations in order to analyze their readiness towards any crisis and tries to find the comprehensive approach towards such crisis in order to find the most suitable role plan which becomes suitable if not for all but for almost all sort of organizations. It covers the plans which needs to be adopted by the organizations for the purpose of dealing with various crises and prepare it to face any sort of negative contingency which may face by them in future.

CHAPTER 3
ORGANIZATION READINESS

As the organizations are the open systems, they may not just orient themselves to the future events. One cannot prepare for the unforeseeable or unpredictable catastrophes. However, a failure of the foresight or pre-preparedness is to be regarded as the collapse of precautions. Several studies have already been conducted in this regard.

According to **Mc Caskey**[114], when the uncertainty level is relatively high then directional plan are more plan and thus that's the spot where the flexibility is needed in order to be able to respond effectively to the unexpected changes. High uncertainty and unexpected changes are the basic characteristics and integral elements in the crisis situations.

In a study[115] on the management bodies of organization, it was found only a few corporate managers or management head who really felt that their organizations are ready to face the crisis, the same is also endorsed by this study as per the examples highlighted through Indian perspective. Reilly mainly concentrated on the organization as a whole and not on any individual element of attribute and importance of the working asset i.e., any technology or workman who is expert in any technology majorly used by the organization. Although, people in the management group may come and go, but the organization as a whole can equip itself and can prepare for and survive any crises.

Through the comprehensive study, Reilly listed the six core components in the crisis readiness:

1. The organization's capability to respond quickly to a crisis.
2. The organization's crisis management repertoire in order to make information available to the managers about the organization.

[114] Michael B. McCaskey, *A Contingency Approach to Planning: Planning with Goals and Planning Without Goals*, 17 AMJ 281–291 (1974), https://journals.aom.org/doi/10.5465/254980 (last visited Jul 23, 2020).

[115] The Role of Human Resource Development Competencies in Facilitating Effective Crisis Communication - Anne H. Reilly, 2008, , https://journals.sagepub.com/doi/abs/10.1177/1523422307313659 (last visited Jul 23, 2020).

3. Manager's access to the plans, resources and tolls relating to the organization's crisis management process.
4. The adequacy of an organization's crisis management planning.
5. The media management ability of the organization in the situation of crises.
6. The perceived likelihood of crisis striking the organization.

In the opinion of **Winter and Steger**[116] on any organizational crisis that, in case of significant risk in a project, it may not just stop the project but surely plan for any contingencies to face the strong oppositions at times.

Their study gave following suggestive measures which is to be noted:

1. Try to influence and manage public opinion.
2. Create some understanding relating to the issue.
3. Try to move beyond the traditional adversarial repetitive stances or practices.
4. Always be very conscious about the company's image which can be damaged by the sudden unnecessary reactions and behavior during the campaign.

3.1. COPING-UP WITH CRISES:

According to the literal definitions, the problem of crises seems very dangerous. When crises come with its full potential, organization start facing the serious risk of failure. To eliminate fully these risk is often difficult and the remedies sometimes bring pain to the people directly affected by it. Therefore, it can be inferred from it that it is the far more important and the best way to cope up with the crisis is to avoid it.

Starbucks[117], provided various suggestions in order to cope up with the crises in the efficient manner mentioned below as:

[116] MATTHIAS WINTER & ULRICH STEGER, MANAGING OUTSIDE PRESSURE: STRATEGIES FOR PREVENTING CORPORATE DISASTERS (1 edition ed. 1998).

[117] Paul C. Nystrom & William H. Starbuck, *To avoid organizational crises, unlearn*, 12 ORGANIZATIONAL DYNAMICS 53–65 (1984), http://www.sciencedirect.com/science/article/pii/0090261684900111 (last visited Jul 23, 2020).

- Eliminate excesses- emphasize prescription which put stress on logical consistency, formality, rationality, planning, agreements, stability, hierarchical control and efficiency.
- Restrict implicit assumptions, behaviors and perceptions which are implicit or needs to be challenged or alter.
- Change top level managers, it is necessary to overcome the crises efficiently whenever required. But when such changes implemented, it is to be total and not to be just formally one or two.
- Experiment with the portfolios i.e., it is important to invest in the new market products and technology.

In general sense, crises exist and grows when there are no immediate measures in order to cope with a threat to a system. As pointed out by **Fink** [118] that, “A human system (individual, group, organizations or other) is assumed to be in a state of crisis when its repertoire of coping responses is not adequate to bring about the resolution of a problem which poses a threat to the system of organization”. Therefore, the disaster and severe level of stresses towards which the human being has no ready effective response which constitutes a crisis.

3.2. COMMUNICATION OF CRISES:

Researchers as well as researchers, now a day, are increasingly aware of the potential reduction in crisis situations that comes from the improving of management and organizational communication and the quality and effort.[119].

Already, various researchers have studied and analyzed the need and importance of the crises communication[120]. Their studies inferred and confirms that the crises communication is the very crucial element of crisis management. It is further highlighted in their studies that the irregular or improper communication management. It is further

[118] FINK AND ASSOCIATION, *supra* note 52.

[119] Causes of Disaster: Sloppy Management, , RESEARCHGATE , https://www.researchgate.net/publication/229743442_Causes_of_Disaster_Sloppy_Management (last visited Jul 23, 2020).

[120] FINK AND ASSOCIATION, *supra* note 52.

stated out that the improper communication during the period of crisis may hugely affect the very existence of the organization.

Therefore, through the reference of the above-mentioned studies and researches, it may be inferred that the process of communication management in the organization plays very integral role in order to trace and make prepared to take preventive action to cope up with such crisis situation beforehand.

Crisis communication plays very important role towards the management and to effectively manage the downhill condition of any efficient organization effectively.

3.3. SUSCEPTIBILITY OF CRISES:

An interesting model of the corporate crisis[121], highlighted with the various corporate characteristics which increases or decreases the susceptibility and vulnerability of organizations to crises. Although, they have provided the comprehensive theoretical concepts and theory models and jurisprudence rather than the practical observation based on an empirical observation, but it is also interesting to note that because it tries to attempt to resemble three groups of variables to market performance and susceptibility to the crisis. These groups are:

- Competitive and environmental variables (technology updates, market decisions and market observation, etc.,)
- Managerial characteristics, such as capabilities of an individual and the way to address and management style.
- Attributes of an organization, such as its resources and its overall structure.

Furthermore, it is also noted by **Barton**[122], in his study that there are some of the factors that especially increase susceptibility to crisis. They are mentioned as:

[121] C. F. Smart & I. Vertinsky, *A cross-impact simulation of corporate susceptibility to crisis: The case for organizational reform*, *in* PROCEEDINGS OF THE 11TH CONFERENCE ON WINTER SIMULATION - VOLUME 2 585–592 (1979).

[122] BARTON, *supra* note 56.

1. Opening a new or the enlarged facility where the machinery, body of system and other technical procedures may not be adequately tested.
2. In a satellite location, forming a new division, for the purpose of temporary period in which a communication system may be erratic and the control measures which affects the decision making needs proper refinement.
3. Forming and launching the new or carefully developed products that has received the most careful review in the limited span of time of its testing. But due to because that it has not had wide use, could be susceptible for the breakage, attacked, leakage or any other problem.
4. Forming the place into the International market, possibly placing the organization's goodwill at odds with the local customs and regulations if there has been inadequate review and planning to get assimilate into the community.

3.4. CRISIS AS OPPORTUNITY:

Highly successful leaders and organizations mostly perceives crisis as an opportunity available for the improvement of market reputation, forming a background for change, introducing the latest technologies and related works, doing innovations and introduction on new business models, new products and new theories etc.

Business Crises as an opportunity: lessons learned: Harvard Business press 2009[123]

3.4.1. International Leaders/Organizations on Crisis:

1. Giam Swiegers, CEO, Delloite (Australia):

- Difficult times are opportunities for the leaders to demonstrate what they are made off.
- A leaders' perceptive in the difficult times can mean the difference between communicating opportunity and the communicating paralysis to an organization.

2. Anders Dahlvig, group President and CEO, IKEA Services:

[123] CRISIS AS OPPORTUNITY, CRISIS AS OPPORTUNITY (2009).

- In times of sustained growth and a stable economy and planning and forming the organization's responses at the time of sudden down storm is crucial for the future success.
- Counterintuitively, a well-managed and planned strategy for the growth can separate organization from the competition during the economic downturn.

3. Mary Cantando, founder of WomenBusinessOwne.com:

- It's easy to play the good hand but only a true master can handle a poor play as well.
- Attitude to look for the good in bad situations provide position to explore the hidden opportunities.

4. William Johnson, Chairman, President and CEO, H. J. Heinz Company:

- The knowledge of strengths and weaknesses based on the facts and sound analysis underlies good strategy and efficient management.
- Counter intuitively, it may be important for an organization to become smaller, even temporarily, in order to achieve its strategic objectives over the long term.
- In depending upon the new or counterintuitive strategy, one should over communicate plans to shareholders, stakeholders and constituents who may not understand its benefits.

5. David Brandon, Chairman and CEO, Domino's Pizza:

- Negative changes can be an opportunity for the organization to create successful outcomes.
- One of the finest ways to prepare an organization for the dynamic conditions, particularly when such changes is perceived as the negative, is it to promote the mindset that wants to embrace it.

6. Amelia Fawcett, chairman, Pension first:

- The capability to make the decisions is practically tested when those decisions are very difficult, not popular and it is subject to criticism.

- Long term strategic management goals can provide ways and fortify convictions in the rightness of decision.

7. Paul Anderson, Chairman Spectra Energy:

- While dealing with a new or different situation, do not assume that you have all answers.

8. Robin Chase, Founder and former CEO, Zipcar:

- In order to trace and alter the failures, as well as to amplify the opportunities, it is important that an organization perceive itself as a learning company.
- Do not reject, avoid or to ignore mistakes or failures, but to accept and correct them as quickly as possible, regardless of short-term discomfort and fear.

9. Ken Freeman, Former Chairman and CEO, Quest Diagnostics:

- In the period of the poor product performance, getting workers of an organizations focused on the customer is a key to return to the profitability.
- Leaders or the top level management of an organization must act inventively and positively to reach their employees and articulate a broad vision in order to encourage and make their active participation to customer oriented or focused change.
- Employee or workmen satisfaction produces the ultimate customer satisfaction, which in turn ultimately yields increased profitability and improved shareholder satisfaction.

3.4.2. National Leaders/Organizations on Crisis:

a) S. B. Waghmare, Managing Director, Suyog Autocast Pvt Ltd:

- Crisis is an opportunity to alter the culture of management and create a sustainable long-term organizational opportunity.

b) Sachit Nayak, Finance Director Eaton:

- Crisis is nothing but the understanding of a right time to create a positive dynamic conditions.

c) Dinesh Deo, Plant Head Saint Gobain Sekuritat, Chakan:

- Crisis is the results of mismanagement of various facet of business of an organizations and failure of weak links in the technical systems

d) Darshan Shah, CFO Kalyani Lehmerz:

- Crisis is the failure of long-term investment planning, which required for growth and sustenance of business.

e) D. A. Bhargav, Radheya Machining Limited:

- Crisis is an outcome of understanding the gap between the organizational potential and our own capabilities.
- Market is always unlimited and endless but our limitations to develop the capabilities to capture the opportunities leads to any form of crisis in the organization.

f) Supriya Badve, Director Badve engineering Limited:

- Crisis is nothing but failure to understand the “Now” and poor or weak response to “Now”.

g) Dilip Palve, Chief Operating Officer, Victor Gaskets India Limited:

- Crisis is an outcome of the priority for any unplanned activities, lack of trust in the supply chain and presence of invisible damage or breaks in systems of an organization.

h) S Sridhar, Head, Lucas TVS, Chakan Plant:

- Crisis is an adverse space between the organizational performance and our working performances.

3.5. Organizational Environment:

Broadly, the organizational environment is the combination of both the external factors and the internal factors, controllable and non-controllable factors. Internal environment is nothing but the resources where the company has direct control and the factors can be managed easily. The internal environment mainly consists of technology, human resource products and the process, source of finance, assets, the overall internal structure of the organization etc.

External organizational environment consists of fiscal and monetary policies of government, political interference and policies, the actual purchasing power of the customer and national state of economy as well as the performance of industry and potential market, various types of competition and global competition indexes, legal and political framework, product life cycles and demands of the customers etc.

Table 3.5.1. Types of Organizational Environment[124]

Internal Factors	External Factors
Technology	Competition among the organizations
Manufacturing the machinery	Governmental Policies
Human resources	State of Economy
Terms and Conditions	Social Responsibilities

3.5.1. External Factors of Crisis in the Organizational Environment:

a) Crises relating to Market Competition:

- ➢ Lethal rivalry
- ➢ Business Potential Contraction

[124] Organizational Environment | Types of Environment - Roarwap, , https://www.roarwap.com/business-environment/organizational-environment/ (last visited Jul 23, 2020).

- Reduction in profit margin
- Low rate of product's life cycle
- Abnormal changes in customers' demand
- Threat from the easy available substitute
- Huge number of product varieties and small volume demand from customer
- High chances of product obsolescence

b) Crises relating to Governmental Policies:

- Uneven delay in project approvals
- Unnecessary changes in required specification
- Uncertain future course of action
- High inconsistent monetary and fiscal policies
- Difficulties in Taxation planning
- Unnecessary restrictions on growth
- Restricted areas of operation
- Restriction in capital formation
- Limited product varieties and high level of volume demand dynamisms

c) Crises relating to the relative economy:

- Negative change in inflation rate
- Market operation stagnation
- Increased borrowing cost
- Reduction in consumption
- Shorten demand and irregular supply
- Sluggish product demand
- Lack of infrastructure

d) Crises relating to social aspect of organization:

- Goods and services not accepted by the society
- Products are opposite of culture of the society

- The production and consumption rate mostly decided by the dominant society

3.5.2. Internal Factors of Crisis in the Organizational Environment:

The below mentioned factors shows various forms of crises faced by the organization relating to change in the internal environment. Internal organizational environment is mainly based on the combination of various resources which is utilized by the organization to improve internal productivity and cope up effectively with the various crises frequently faced by organizations.

a) Crises relating to Research and Development:
   - Uneven delay in production cycle
   - Lack of proper system testing facilities
   - Perishable output of product or service
   - Lack of proper investment for extensive research
   - Governmental restrictions on the goods and services

b) Crises relating to Technology:
   - Under-utilization or idle capacity of machinery and equipment
   - Lack of financial capacity to update new technology
   - Lack of technical skills to perform and operate latest machinery and equipment
   - Rise of maintenance cost due to the use of high-end technology
   - Quick changes in technology and time lag to cope-up with new technology
   - High cost of hardware tools and useful equipment associated with new technology
   - Requirement of sufficient volume for the proper utilization is high

c) Crises relating to Manufacturing the machinery:
   - Outdated machines and equipment
   - High risk of breakdown and downtime
   - Low level of output cycle
   - Rejection of process and wastages of resources

- Operational inefficiencies
- Issues relating to minimum quality maintenance

d) Crises relating to Human Resources:

- Lack of technical skills
- Non-adaptive to new change and to acquire new-skills
- Vibrant industrial relations
- Uneven strikes by labour union and non-cooperation movements
- Discriminatory and uneven employee policies and practices
- Exploitation of workmen

e) Crisis relating to company policies:

- High attrition rate
- Higher cost of production
- Lack of financial resources
- Financial loss
- Contraction of working opportunities
- Delayed completion of targeted projects

Approaches towards external organizational environment[125]:

Mostly, a crisis caused by the external organizational environment is uncertain in nature. Its effect is very fast and it may create the long lasting impact on the organization. It may create an alarming situation and poses a big question mark on the survival of such organization. Normally, there are very few and weak signals about the crisis and people fail to recognize patterns to trace the signals. Such failure to receive signals and response related to severe crisis for the organization.

An efficient approach towards crisis management, well trained to deal with the crisis and reduce the effect on the people affected and relatively involved. Harvard Business School has provided a generic approach towards the effective crisis management.

[125] Kweku Ewusi-Mensah, *The external organizational environment and its impact on management information systems*, 6 ACCOUNTING, ORGANIZATIONS AND SOCIETY 301–316 (1981), http://www.sciencedirect.com/science/article/pii/0361368281900106 (last visited Jul 23, 2020).

Crisis has many initiation points and these are often unique to an organization's line of working. A major crisis will affect the entire organization and may also lead to collapse. The top level management must act quickly to recognize the source of crisis, contain it and resolve the crisis with much less amount of damage.

Some crises can be considered as a fire and they start in small-unaddressed area. If the smoke is smelt and identified at early stage, the fire can be soon averted. But, if unnoticed these small fire can grow into catastrophic infernos.

Every crisis is an expensive affair for the organization. Even when such crisis is resolved and managed it effectively; there will always be a cost overrun in terms of money, market, reputation and also for employee morale. But, also these costs are learning opportunities for organizations. Smart organizations learn from every experience and apply the leanings for the future challenge. Continuous learning helps to become wiser and more effective. These learnings should be a base for avoiding and / or preparing for future crisis.

3.6. MASTERING THE SKILLS TO PREVENT CRISES:

In order to master the skills to prevent crisis, an organization must possess effective crisis management model to deal with any form of crisis beforehand. First of all, it is crucial to deal with the crisis relating to the external environment. The external organizational environment can create a long lasting effect on the working of any organization and which may also result in turn due to which, stakeholders may be dissatisfied. Continuous evaluation of positive changes in the external organizational environment and assuming the probable impact on the regular performance which should be ongoing activity in any organization. This approach may help any organization to reduce the impact of unseen perils relating to any crises.

The suggestive steps to create positive approach towards external organizational environment crisis management process are:

1. Taking stock of potential crises
2. Avoiding the avoidable damage
3. Planning for contingent conditions

4. Crisis Recognition
5. Crisis Containment
6. Resolution of Crisis
7. Mastering the Media
8. Learning from previous experiences

Taking stock of potential crisis[126]**:**

- Certain specific changes in the environment of an organization can induce crisis. These changes may be the change in any government policy, working environment, fiscal and monitory policies changed by the government in less time.
- Any price control regulations imposed by government, changes in tax bodies and structures can create impact on selling and profitability of an output line and it may be difficult to sustain for long in competition.
- Negative economic and market forces- It's a common saying that, "A rising tide lifts all boats", all organization initially does well during good economic times and similarly, when the tide goes out, all the boats go down. The fortunes of all organization are to some extent bound to carry the up and down of economic cycle. Down phases are particularly dangerous to the organization facing the high fixed costs. Some organization find themselves exposed to in favour / out of economic cycle.

Identification of Potential Crisis[127]**:**

- The overall audit of an environment of organization should be a regular practice such like any other statutory audits mainly conducted by the organization.
- Extensive research should be conducted in order to identify the predominant change in market forces and prevalent expectations of customer.

[126] Dealing with the Crisis: Taking Stock of the Global Policy Response, , RESEARCHGATE , https://www.researchgate.net/publication/228125690_Dealing_with_the_Crisis_Taking_Stock_of_the_Global_Policy_Response (last visited Jul 23, 2020).

[127] Identifying A Crisis and Managing it Effectively, , MELISSA AGNES - CRISIS MANAGEMENT KEYNOTE SPEAKER (2012), https://melissaagnes.com/identifying-a-crisis-and-managing-it-effectively/ (last visited Jul 25, 2020).

- Closely observe the governmental policies and suggested changes in the relevant legislative systems needs to be studied thoroughly.

Prioritizing the Potential Perils[128]:

It is always said that people are not so good at dealing with sudden risks. They are afraid of so-called severe risky events even though having less probability of its occurrence but they have general tendency of ignorance attitude towards such risks, which have higher probability of its occurrence. A systematic approach towards evaluation of risks and calculation of its probable impact may surely help to develop the effective crisis management approach.

Generally, various market experts apply the simple quantifiable function called as the expected value which can be used for the purpose of prioritizing the present and future crisis management actions.

E(X) denoted for expected value is the anticipated outcome of an event (E) times the probability of the event occurring (X). This simple consequential equation weights the anticipated outcome through the assumption by calculating the probability that it will happen.

Avoiding the avoidable damage[129]:

The avoidance of any crisis can be as regular as the internal financial control mechanism that prevent embezzlement or the squandering of any organization resources. At the same time, it can be as complex as a production management. Manufacturing companies can avoid costly lawsuits customer boycotts and bad press by giving greater attention to production management.

[128] Taking Stock of Potential Perils: What Could Go Wrong? | Harvard Business Publishing Education, , https://hbsp.harvard.edu/product/6419BC-PDF-ENG?Ntt=&itemFindingMethod=Recommendation&recommendedBy=BH658-PDF-ENG (last visited Jul 25, 2020).

[129] Norman R. Augustine, *Managing the Crisis You Tried to Prevent*, HARVARD BUSINESS REVIEW, 1995, https://hbr.org/1995/11/managing-the-crisis-you-tried-to-prevent (last visited Jul 25, 2020).

Prepare a systematic model for the crisis avoidance. A positive and active approach towards crisis, regular overall audit organizational environment, market condition research to understand the current demand and understanding the requirements of changes in legal systems which will help to prepare effective crisis management plan and impact on working output of an organization can be minimized.

Planning for Contingent Conditions:

Planning for the Contingent conditions involves organizing and making as many optimum decisions as before a crisis occurs in an organization. Pre-crisis planning provides organization the time required to consider every possible options. The management and technical team can think through, discuss merits and demerits of various reactions, and test their preparedness of organization. Most of the time, some risks are potentially more dangerous or costly than others. It is beneficial to use probability adjusted risk assessment in order to determine which all risks can effectively have neutralized through the technical or managerial actions or through any form of insurance. As, many crises began as a small problem. By heeding the signals of prevalent creeping crises, one would be able to neutralize them before they grow in the dangerous form and become expensive. Some crises are self-inflicted by the organization. These can be mostly avoided by the thoughtful anticipation of the consequences of policies and actions of the organization.[130]

Crisis Recognition:

An important aspect of any crisis management and its first step is Crisis recognition[131]. The technical or management teams can work more effectively in the case of early recognition of crisis rather than midway of crisis. These teams needs to be get prepared to address before the too much damage is done. Many forms of crises begin as little embers that gradually grow hotter, eventually ignite and burn everything around them. When crisis begins with small, organization may fail to recognize but by the time they

[130] Kerstin Eriksson & Allan McConnell, *Contingency planning for crisis management: Recipe for success or political fantasy?*, 30 POLICY AND SOCIETY 89–99 (2011), https://doi.org/10.1016/j.polsoc.2011.03.004 (last visited Jul 25, 2020).

[131] Gordon L. Lippitt & Warren H. Schmidt, *Crises in a Developing Organization*, HARVARD BUSINESS REVIEW, 1967, https://hbr.org/1967/11/crises-in-a-developing-organization (last visited Jul 25, 2020).

notice what is actually happening, the crisis has already grown to the point that it is dangerous and ultimately difficult to contain.[132]

Containment of crisis to prevent bad situation from getting worst[133]:

An unaddressed crisis and left without any change, some of the crisis will move from bad to even worst. A crisis caused in any single area can create a crisis in another area if not checked promptly. Containment of the crises is defined as the planned decisions and actions that aims to keep crisis from growing and becoming worse. Containment of crisis is the identification of specific problem and figure out the initial plans and ideas to stabilize the situation and to prevent the crisis from growing it into worse.

Resolution of Crisis[134]:

Crisis Resolution is an important aspect towards the crisis readiness and to be considered as a sequential approach, which a crisis technical or management teams needs to understand and implement it effectively.

The approach includes:

- Move quickly and be resilient
- Gather relevant facts continually
- Communicate relevant informations relentlessly
- Speedy document action
- Use different project management techniques when appropriate
- Be a reliable leader
- Declare the end of crisis after confirmation

Mastering the Media[135]:

[132] Recognition in a time of crisis | Employee Rewards and Recognition Programs, , ACHIEVERS , https://www.achievers.com/media/recognition-in-a-time-of-crisis/ (last visited Jul 25, 2020).

[133] Norman R. Augustine, *Managing the Crisis You Tried to Prevent*, HARVARD BUSINESS REVIEW, 1995, https://hbr.org/1995/11/managing-the-crisis-you-tried-to-prevent (last visited Jul 25, 2020).

[134] Shangharsha Thapa, *Crisis resolution* (01:23:41 UTC), https://www.slideshare.net/Shangharsha/crisis-resolution (last visited Jul 24, 2020).

[135] How to Handle the Media During a Crisis | CIO, , https://www.cio.com/article/2438594/how-to-handle-the-media-during-a-crisis.html (last visited Jul 25, 2020).

Communication is an important tool for every crisis containment team, in every stage of the crisis. Communication through the media i.e., newspapers, television and the radio must also be used to accurately prepare the crisis in the stakeholders' mind, the message should be accurate and succinct. It should be current organization's point of view and include facts that support it.

Learning from previous experience[136]:

Mostly, growing organizations keeps on learning from their all types of previous experience. It is essential to note that, learning during the ongoing process of crisis containment should be continuous in nature. The systematic record should be maintained properly at each level during the crisis containment about the problems faced, suggested solutions/ preventive measures and implemented. The maintained document should also record what exactly went right and what went wrong in the entire process after implementation of any approach.

Thus, the organization readiness equates not only to just a vigilance, for example in the form of keeping eyes open 24 hours is just not enough, but it may also include the appropriate readiness of required resources. A well prepared, multifunctional technical and management teams must be organized and prepared to deal with all the aspects of any prevalent crisis. In addition to this, the crisis simulations and pre-preparedness enables the management to understand the conditions, what can happen, which steps needs to be taken, and whether such organization is truly prepared to deal with any such crisis beforehand or not.

3.7. READINESS TOWARDS CYBERSECURITY CRISES:

In the present times, almost, all the organization are in a way based on the cyberspace for one or another business requirement which make them efficient in connecting with the customer miles away and help them to provide them quality product

[136] (3) (PDF) Learning from Crisis: A Framework of Management, Learning and Implementation in Response to Crises, , RESEARCHGATE , https://www.researchgate.net/publication/40823576_Learning_from_Crisis_A_Framework_of_Management_Learning_and_Implementation_in_Response_to_Crises (last visited Jul 25, 2020).

or services. Cyberspace plays very important role for moving any business and make organizations up-to-date with any prevalent technology which is required to be equipped by the organization.

Many technologies based organizations in India have their relevant records either on cloud or they possess important business mails or have personal details of clients saved on their website which makes them always connected with cyberspace. So, it is crucial for such organizations to maintain the equal or even high level of cybersecurity towards such data because if such data may get lost or stolen or breached or the system which possess all the relevant data breakdown, then, these incidents may lead to the organization towards the collapse.

There are certain basic elements which is to be acquired by any organization for the purpose of pursuing and preparing self for the stronger cybersecurity, i.e., vigilant, secure and resilient approach[137]. For the purpose of sufficient readiness, an organization should strive to become:

1. **Vigilant Approach:**

Vigilance demands that everyone should be aware of how they could introduce the organization to cyber risks through their systems and devices, social media and through any online official conduct. A vigilant approach relies on gathering all the threat-related intelligence and gauging the range of threats that could harm the output of organization. This information also enumerates about the mechanism for cyber threat monitoring. In addition to that, appropriate policy development, availability of machinery, related training, and fair accountability regarding cyber incidents each play a key role in maintaining vigilance.[138]

2. **Secure Approach:**

A secure organization provides preference to the value of digital assets, with a focus on what is really most important to the organization. All data does not create equal, nor is

[137] Using a Secure, Vigilant and Resilient Approach to Cyber Risks - Risk & Compliance Journal - WSJ, , https://deloitte.wsj.com/riskandcompliance/2016/06/30/using-a-secure-vigilant-and-resilient-approach-to-cyber-risks/ (last visited Jul 24, 2020).

[138] *Ibid.*

it the practical or possible for any organization practically to provide complete security for all their data. By just prioritizing the value of digital assets, technical and management team can allocate optimum resources according to the value of such available digital assets, with the goal of obtaining a high level of security that actually corresponds to their security value.[139]

3. **Resilient Approach:**

A resilient approach taken by organization targets to minimize the effects of an incident on the organization and its stakeholders while speedily restoring the operations, credibility towards customers, and the security. Swift detection of cyber crashes or incidents and well-structured comeback recovery plans can usually control the damage. Recovery plans should be provided in order to clear roles, responsibilities, and actions to deal effectively with damage and to reduce future risk, remediate the crisis situation, and return to its normal operations.

An organization ready and prepared beforehand towards any challenges possess all these above mentioned elements can be considered as at least ready to face any crises in the organization especially any technological crisis. A secure, vigilant, resilient organization has all three phases of cyber risk containment covered.[140]

Furthermore, cyberattack response programs require coordination in mainly five key areas: governance, strategy, technology, risk and compliance and remediation[141]. They all are briefly discussed as:

1. Governance:

Governance provides the way of organizing and managing the response team of an organization. It ensures the program coordination across the technical areas, documentation of all the policies, procedures, and the incidents, and clear communication roles,

[139] *Ibid.*
[140] *Ibid.*
[141] How to build an effective information security risk management program, , HTTPS://BLOG.NETWRIX.COM/ , https://blog.netwrix.com/2018/08/02/how-to-create-an-effective-information-security-risk-management-program/ (last visited Jul 24, 2020).

responsibilities, and protocols. Governance takes to provide response strategy with goals and provides mechanisms for cross-functional communication process.

2. Strategy:

Response strategy enumerates how you lead, prioritize and efficiently communicate during incident response and crisis containment. Organizations should align response strategy with the organization's values and responsibilities. A well prepared strategy provides a cost effective, well-resourced, organization-wide approach to addressing cyber incidents. This reduces tunnel vision in the response planning and reduces the adverse impact to operations and revenue.

3. Technology:

The Information Technology and cybersecurity teams creates and implement mechanisms for the purpose of identifying, detecting, monitoring, responding and to recovering from a cyber-incident or crisis. IT employees create the needed architecture, and IT working to maintain systems that are resistant to attacks.

Technical forensic and investigative methods are vital to keeping evidence safe and analyzing control failures, security lapses, and any other conditions related to the crisis. In addition to that, organizations should install both the proactive and responsive technology solutions to deal with the future cyber related incidents.

4. Risks and related compliances:

Risk and compliance functions related to such risks should be assessed and managed through the regulatory compliance elements of the incident and response to the crises, including interfacing with the legal counsel, law enforcement and regulators. The keys are to be able to comply with minimum requirements and to enumerate such compliances. For example, after any breakdown or incident, investigative processes and responses must be properly documented in order to demonstrate the adequacy of both.

5. Remediation:

The remediation process needs to remove or significantly reduces root causes of crises and return businesses, functions, IT related machineries and stakeholders to a secure operating environment.

When it comes to incident and crisis containment, readiness is an evolutionary state of affair for any organizations. What the organization were ready for yesterday may be the last thing cybercriminals have in mind today. Indeed, organizations cannot really know the specific source or target of the next attack.

But these organizations can gauge risks based on the value of their all the digital assets and the impact of their systems being compromised. They can gauge likelihood and they can ready the organization for the effective response and recovery and make them sufficiently ready through the said approaches and measures if taken carefully by these organizations. The current trends have created paradigm shift from workmen excellence to the technology excellence. They are becoming important assets for the organizations, so it is important for them to maintain high security for such valuable assets and to make themselves prepared for all the upcoming dangers and loses through right approaches and proper management process models in order to assess the organization readiness towards such challenges and analyze the reasonability of actions taken by them towards curbing of such problems. It is also important to analyze the best suitable model for the purpose of containment of crisis in order to find the appropriate models towards the fulfilment of crisis management.

The upcoming chapter tries to cover the exhaustive concepts, explanations and various models relating to the crisis management process which can be analyzed and adopted by the organization who faces regular threats of crisis as per their conditions and overall structure.

It also tries covering the importance of crisis management models suitable for almost every technology based organization to not only to cope-up with the technology related crisis but also make the working pattern of organization disciplined at the same time flexible as per the conditions of market.

CHAPTER 4

CRISIS MANAGEMENT

"A crisis is an opportunity riding the dangerous wind"

- **Chinese Proverb**

Momentarily, the Crisis Management is becoming one of the new steps of precaution towards maintaining the organization's discipline. In this area, acquiring the adequate knowledge in this field is becoming a must for the technical and management team of the today's organizations. Planning for a crisis is an art of removing much of the risk and uncertainty to allow you to achieve more control over your own destiny[142]. Crisis management sees a crisis as an isolated event that can be analyzed in terms of causes, consequences, caution (prevention or minimizing the impact) and response to the crisis[143].

The term 'Crisis Management' has been defined in various ways in order to understand its concept and its importance for the organizations:

Experts**[144]** explained that 'Crises management is not just straight forward action of rules, regulations and procedures to be followed by the organization. It possesses full range of thoughtful processes and the steps that assumes the complex nature of crisis real and perceived'.

As per **Mitroff**[145], 'Crisis Management is concerned primarily with the series of internal and external forces that can result in collapse of the existence of an entire organization. The outside cyberattack on the on the latest technological system which may cause the loss of whole firm may damage the reputation of whole firm. So, the external saboteurs can also threaten an organization, perhaps by bypassing the whole system security of the organization.

[142] FINK AND ASSOCIATION, *supra* note 52.

[143] Paul Shrivastava, *Crisis theory/practice: towards a sustainable future*, 7 INDUSTRIAL & ENVIRONMENTAL CRISIS QUARTERLY 23–42 (1993), https://www.jstor.org/stable/26162560 (last visited Jul 24, 2020).

[144] THE HANDBOOK OF STRATEGIC PUBLIC RELATIONS & INTEGRATED COMMUNICATIONS, *supra* note 57.

[145] Ian I. Mitroff, Terry C. Pauchant & Paul Shrivastava, *The structure of man-made organizational crises*, 33 TECHNOLOGICAL FORECASTING AND SOCIAL CHANGE 83–107, https://www.academia.edu/23876994/The_structure_of_man-made_organizational_crises (last visited Jul 24, 2020).

At the core, the crisis management can be considered as a series of ongoing, multilayered, interrelated assessment or audits relating to various kinds of crises and forces that directly threatens the products, services, manufacturing processes and the surrounding environment of the organization. Crisis management encompasses the design and effective implementations of plans, procedures and regulations for the purpose of detection of, prevention of, preparation for, containment of and recovery and learning from the key crises'.

An efficient Crisis Management Plan must consist of a full range of thoughtful and insightful processes and steps that anticipates the complex forms of crises beforehand built upon the rational expectations on it about how that crisis will manifest itself and how on it the organizational response would be[146]. The results of crisis may not be confined towards the organization but where the crisis manifests itself but also has its impact on all sort of stakeholders related to it, most probably with a high amplifying effect.

4.1. PHASES OF CRISIS MANAGEMENT PROCESS:

There are four stages of the Risk and Crisis Management[147]: The aim of this section is to provide one exhaustive framework, the Four R's approach adopted by many organizations to show how destinations and even a small organization can effectively manage the four distinct phases relating to a crisis: i.e., first is, Reduction- detecting early warning signals; second is, Readiness- preparing plans and the continuous exercises; third is, Response – it is for executing the technical, operational and communication plans in a crisis situation; and the last one is, Recovery - for the purpose of returning the organization to normal after a crisis. The focus of this part is expecting the unexpected incidents, and to be prepared beforehand. This section emphasis heavily on the concept of crisis risk management and the response strategies from various fields connected to the technology, especially the areas of emergency areas of an organization related to cyberspace.

[146] THE HANDBOOK OF STRATEGIC PUBLIC RELATIONS & INTEGRATED COMMUNICATIONS, *supra* note 57.
[147] Tourism Risk Management for the Asia Pacific Region, , RESEARCHGATE , https://www.researchgate.net/publication/273062770_Tourism_Risk_Management_for_the_Asia_Pacific_Region (last visited Jul 24, 2020).

A well-defined crisis management program developed, analyzed and implemented by an organization in advance can help not only to the single department but also to an organization to grow and ultimately uplift the market of the country and their organization shine in what may otherwise be a time of dark disaster for everyone involved. The most effective crisis management potentially occurs where a potential crisis is clearly detected and dealt with quickly – before it takes a form of a crisis. Technology based organizations with no crisis management system in place may inevitably have to deal with an unforeseen danger which may leads to its collapse.

Many times, the developing continuity plans may seem like a daunting task to the management, but in reality it is an essential and common-sense procedure based on established management, intuitions, planning based on them and decision-making theory. It involves the process of identifying the potential strengths and weakness of the organization, designing the contingency plans in order to mitigate the potential losses and understanding how the key stakeholders and the media are likely to react when they find out about a crisis in any organization.

Identifying this potential crisis is the key to enable the process of crisis management and further seeking the approaches in order to reduce its impact. The organizations need to evaluate their crisis exposure and create the strategic, tactical and communication plans so as to be able to get prepared psychologically and physiologically for the outcomes and stresses that crisis incidents may impose upon the organization. This may restrict a potential crisis in the making also. Response over it becomes apparent whether the reduction and the readiness phases have created the continuity and contingency plans which all are effective.

Every successful instance of the crisis management process has featured the precise implementation of the operational plans saving not only property but also lives of the team members; and the controlling and maintaining the communications objectives which saves both, the image and the business of the organization. The effective preparedness in both of them is essential.

The crisis divided into three phases, namely:

1. Pre-Crisis phase;

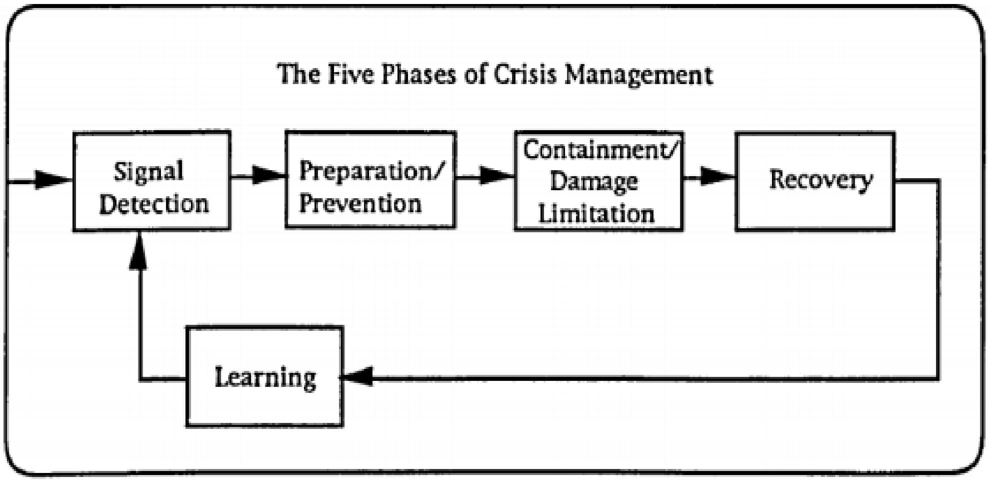
2. Crisis Response phase; and

3. Post Crisis phase.

The elimination of known risks that could possibly lead to a crisis and preparation towards the foreseen crisis needs to be planned under the process as a Crisis Management Program (CMP) for the organization during the Pre-Crisis Phase including preparing, planning, selection and training the CMP team (including members for technical assistance, legal securities, financial operations and human resources) and just testing the plan and the team.[148]

Further, **Mitroff and Pearson**[149] have divided the process crisis management in five phases. The Figure enumerated below is a diagrammatic representation of the same phases.

Figure 4.1.1. The Five Phases of Crisis Management[150]


The Five Phases of Crisis Management
Signal Detection
Preparation/ Prevention
Containment/ Damage Limitation
Recovery
Learning

[148] Developing Concise Key Messages A key step in effective communication is to | Course Hero, , https://www.coursehero.com/file/p6pnniv/23-Developing-Concise-Key-Messages-A-key-step-in-effective-communication-is-to/ (last visited Jul 24, 2020).

[149] Christine M. Pearson & Ian I. Mitroff, *From Crisis Prone to Crisis Prepared: A Framework for Crisis Management*, 7 THE EXECUTIVE 48–59 (1993), https://www.jstor.org/stable/4165107 (last visited Jul 24, 2020).

[150] *Ibid.*

In addition to the earlier theory, one more crisis management theory exists which has the four-phase crisis management model process that mainly covers: the issues management, planning-prevention, the crisis and the post-crisis created by the scholars[151].

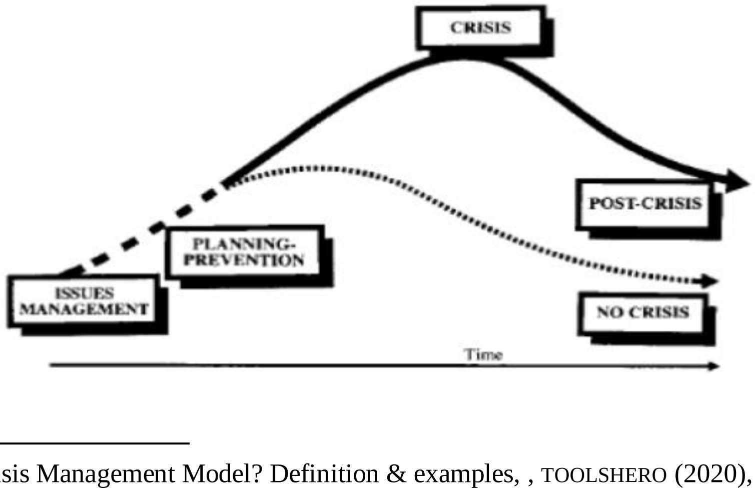
Issue Management Stage: It represents the first task of a crisis communications managing team that suggests the auditing of the organizational environment for the single issues that may affect an organization in the near future; the process of collecting relevant data on crisis and carefully evaluating them; and forming appropriate strategy in order to prevent the crisis or just to redirect its course.

Prevention Stage: The next stage guides for the research of typical related technologies by taking careful feedback in order to acquire sufficient knowledge about organizations constituencies and to determine the message outlets that would be used in implementing the crisis communications plan.

The crisis stage: It deals with the decision taken by leaders on technical grounds which lead to a fall in the value of the organization in the market.

Post Crisis stage: it deals with how the top management responded to the stakeholders' advice and demand, how they judged the crisis response strategy and how they evaluated and implemented it.

Figure 4.1.2: Four Phases of Crisis Management Process by Gonzalez-Herrero and Pratt (1995)[152]



[151] What is the Crisis Management Model? Definition & examples, , TOOLSHERO (2020), https://www.toolshero.com/management/crisis-management-model/ (last visited Jul 24, 2020).
[152] *Ibid.*

4.2. CONTINGENCY PLANNING THEORY:

Preparing contingency plans[153] in advance, as part of a crisis management plan, is the first step to preparedness for a crisis ensuring by an organization. That has to be tested by exercises and mock drills before a real crisis situation knock the door. There must be a designated spokesperson may be from a pre-decided crisis team to speak publicly during a crisis. The plan should indicate how quickly each function should be performed in the first hours when a crisis breaks as it is crucial. Drafts should be there in place to make a statement externally as well as internally, for accuracy to avoid any backfire and exacerbation of the situation. The contingency plan should contain information and guidance to help decision makers for considering the short term and long-term effects both of every decision.

4.3. THE COMPLEXITY LENS:

It has been seen from an organization's scientific perspective, it can be easily understood that why the traditional approach towards the crisis response through the linear cause-and-effect Crisis Management Program is ineffective as an organization as a complex system is sensitive towards the initial conditions and also unpredictable. Due to the dynamic changes in both the internal and the external organizational environment, the initial situations of a crisis constantly change with the significant effects on the organization's life fitness landscape[154].

Generally, the Crisis Plans are too rigid and fail to adapt to the higher performance phase, thus, when programmed for the certain condition becomes ineffective under some other conditions. The system is able to alter the internal structure and organization and the behavior of an individual element from the learning's through its environment over the

[153] Contingency planning for crisis management: Recipe for success or political fantasy?, , https://www.tandfonline.com/doi/full/10.1016/j.polsoc.2011.03.004 (last visited Jul 24, 2020).

[154] Crisis Management or Crisis Response System?: A Complexity Science Approach to Organizational Crises | Request PDF, , RESEARCHGATE , https://www.researchgate.net/publication/235280200_Crisis_Management_or_Crisis_Response_System_A_Complexity_Science_Approach_to_Organizational_Crises (last visited Jul 24, 2020).

certain period of time[155]. The system also directly or indirectly influences the other organizational sub-systems and also the external environment[156], in order to justifying the relative complex co-evolving system. Crisis planning, in this light, simply defines the rules of the system's interface interactions and the "selection environment" through which it generally operates[157].

4.4. Purpose of Crisis Management:

There are several reasons for as to why an appropriate crisis management is essential for any technology based organization. Unless, such organizations have the formal Crisis Management and Crisis Response programs learned, analyzed and implemented, the crisis problems will not require small plans and cannot be eradicated through a short-term solution. As already, previously mentioned that, a crisis may transform from a minor incidence to a very significant, large and complex issue that really may require large amounts of time and resources by the organization towards containing it efficiently. Also, it may threaten not only to the organization or an individual itself but to the society in which it was formed and operates, therefore, there is no other chance than to create a safeguards and protocols that can help people to adequately response to a crisis. The most important purpose of crisis management is the Survival. It is not always possible to get saved from a crisis; therefore, thus, Crisis Management helps an organization, an individual or a country to survive in and after the crisis.

Other reasons for Crisis Management are meant to minimize negative reactions as they could restrict any organization from effectively recovering from their disaster, either for a reasonable time or even permanently; in order to safeguard the assets f organization

[155] Knowledge-Based Innovation Systems and the Model of a Triple Helix of University-Industry-Government Relations, , ResearchGate , https://www.researchgate.net/publication/2521844_Knowledge-Based_Innovation_Systems_and_the_Model_of_a_Triple_Helix_of_University-Industry-Government_Relations (last visited Jul 24, 2020).

[156] Stuart Kauffman & William Macready, *Technological evolution and adaptive organizations: Ideas from biology may find applications in economics*, 1 Complexity 26–43 (1995), https://onlinelibrary.wiley.com/doi/abs/10.1002/cplx.6130010208 (last visited Jul 24, 2020).

[157] The Coevolution of New Organizational Forms, , ResearchGate , https://www.researchgate.net/publication/228593418_The_Coevolution_of_New_Organizational_Forms (last visited Jul 24, 2020).

as the products, facilities, equipment and system can all be threatened by a crisis situation; to minimize the technical and financial losses as only a small portion of such possible losses can be protected through the insurance and savings but the bigger loss of market share through lost shares and customers and broken product or service allegiance will have long lasting impact on the organization.

Figure 4.4.1. mentioned below highlights the crisis management model[158], addresses the basic issues relating to crisis management such as crisis typology, crisis phases, stakeholder management and crisis resource management highlighting and enumerating the distinct forms of crisis management functions in each phase. The model clarifies that how crisis management takes place, prior to the occurrence of a crisis. It is important to emphasize that in today's world if one is not in a crisis one is in a pre-crisis situation. A crisis provides more opportunities than threats if one is crisis-prepared.

The framework has added the learning of the organization as an important aspect of the Crisis Management. This framework gives the action plan and strategic linkages for the effective crisis management. This framework helps to create linkages between the external or internal business environment, and provides a systematic action plan for effective crisis management.

As the technology grows, it has the great potential which may expose any organization to a variety of damage, such as social media breakdown, ransomware scams and bad alerts that may spreads for instance, wildfire. In this digital world, technology has enabled the level of crises to emerge and grow even more rapidly and through this, organizations must be able to access and activate an appropriate and potentially sound crisis management plan quickly and confidently in order to keep pace with the rest of the competition as well as to maintain internal discipline of the organization.

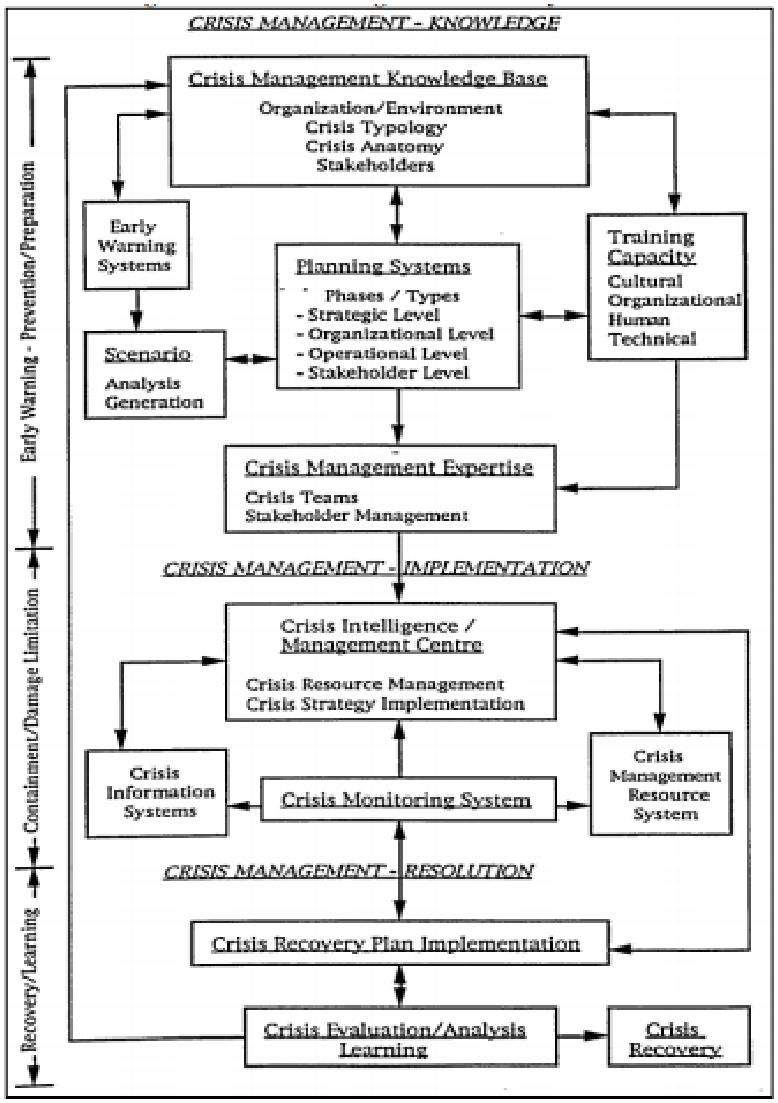
Considering the consequences of a slow crisis response at the organization. Online outrage may grow over a negative news article or a damning social media live video streaming. The clients may just get fed up waiting for the response of information about a

[158] Guilherme Guimrães Santana, *Crisis management: towards a model for the hotel industry : an examination of crisis preparedness and stakeholder relationships in crisis situations.*, May, 1997, http://eprints.bournemouth.ac.uk/299/ (last visited Jul 24, 2020).

product recall or even worse, still, the personal information of clients and partners may be compromised by a rapidly growing data breach through the malpractices of hacking or breaking the system of the organization.

Crisis need not strike any organization purely as a consequent of its own negligence or any misadventure. Often, there are conditions where uneven situation is created which cannot be blamed on the organization- but the organization finds out pretty quickly that it may takes a huge amount of blame if it fumbles the ball in its own response

Figure 4.4.1. Crisis Management Model by Santana, 1997[159]


CRISIS MANAGEMENT - KNOWLEDGE
Crisis Management Knowledge Base
Organization/Environment
Crisis Typology
Crisis Anatomy
Stakeholders
Early Warning Systems
Planning Systems
Phases / Types
- Strategic Level
- Organizational Level
- Operational Level
- Stakeholder Level
Training Capacity
Cultural
Organizational
Human
Technical
Scenario
Analysis
Generation
Crisis Management Expertise
Crisis Teams
Stakeholder Management
CRISIS MANAGEMENT - IMPLEMENTATION
Crisis Intelligence / Management Centre
Crisis Resource Management
Crisis Strategy Implementation
Crisis Information Systems
Crisis Monitoring System
Crisis Management Resource System
CRISIS MANAGEMENT - RESOLUTION
Crisis Recovery Plan Implementation
Crisis Evaluation/Analysis Learning
Crisis Recovery
Early Warning - Prevention/Preparation
Containment/Damage Limitation
Recovery/Learning

[159] *Ibid.*

This research provides a new dimension and insights into the research of crisis management with the context of Indian technology based organizations. The current scenario appears to enumerate that, an extension of Indian IT sector to even some more locations other than Bangalore which is considered the Silicon Valley of India; Chennai, which may be deemed as the second largest software exporter after Bangalore; Mumbai, which is also known as the commercial and financial capital of India; Hyderabad, it can also referred to as the Cyberabad with the good infrastructure and potential technological base and the NCR-national capital region is already filled-up with almost all major IT giant's development organizations and quite a few IT start ups across Gurgaon and Noida/greater Noida region) etc. The significant growth has also been witnessed in other areas of Indian states like Orissa, West Bengal, Maharashtra, for instance, Pune, having a good potential to become a major IT hub in India, Kerala, with setting up of India's biggest IT park i.e., Techno park and also various cities of Gujarat which organized and implemented one of the finest model against cyberattacks on the organization of major cities, etc.

The strategic plan may include the functional level decisions for the internal environment crisis and organizational intervention to manage external environment business crisis. The establishment of the working operations back to normal situation is a top priority. This may include contentment of various stakeholders. Organizational learning should be properly documented and kept as a reference to develop and enhance crisis management skills. The learnings should enhance the understanding of effects on business environment and create a team to manage such crisis effectively to create better opportunities towards the business of the organization.

4.5. RELATIONAL MODEL FOR CRISIS MANAGEMENT:

This model is prepared on the specific view of crisis management, that crisis prevention and crisis preparedness are as important as the overall process and the tactical steps to take once a crisis strikes. Furthermore, that the post-crisis cluster of activities has a critical function looping back to preparing for and managing future crises. This model represents group of ideas and not mere sequential steps in the process. The processes are interdependent and sometimes overlapping also. The model is non-linear and there is a sequential loop for refinement of crisis management process.

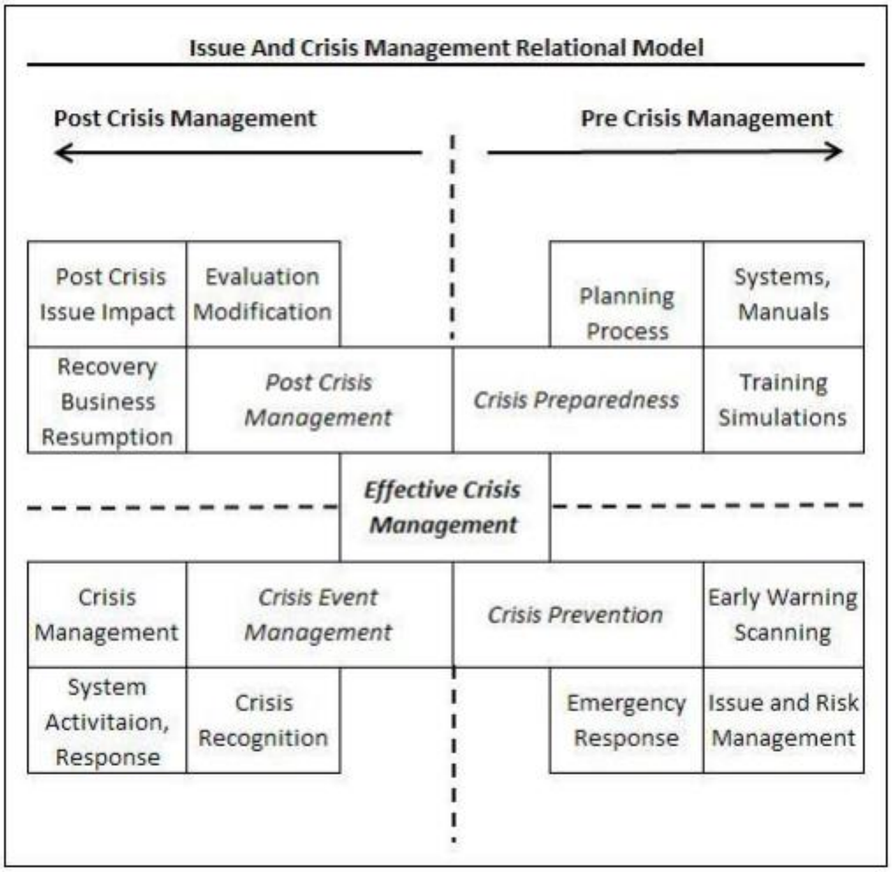


Figure 4.5.1. Relational Model for Crisis Management[160]

It is pertinent to note that the relational model for crisis management as mentioned in the above figure provides tested directions to be followed in the two situations i.e., Pre-Crisis Management and Post Crisis Management which further enumerates the approaches which can be analyzed and followed as per the requirement of the condition faced by the

[160] W. Timothy Coombs, *Crisis management: Advantages of a relational perspective*, *in* PUBLIC RELATIONS AS RELATIONSHIP MANAGEMENT: A RELATIONAL APPROACH TO THE STUDY AND PRACTICE OF PUBLIC RELATIONS 73–93 (2000).

organization, this organization can further adopt this approaches by inculcating patterns mentioned as:

Crisis Preparedness[161]**:**

- Includes putting planning in place, assigning roles and responsibilities, establishing process ownership.
- Includes crisis management infrastructure, equipment, war-rooms, resources and documentation.
- Includes training programs, demonstrations, exercises and live simulations.

Crisis Prevention[162]**:**

- Includes processes such as audits, preventive maintenance, issue scanning, environment scanning, anticipatory management, future studies.
- Includes identification, prioritization, strategy development and implementation.
- Includes infrastructure, documentation and training.

Crisis System Management[163]**:**

- Includes the transition from emergency, objective assessment, early recognition.
- Includes the activation process, system for callout, availability of back-ups, system redundancy.
- Includes strategy selection and implementation, damage mitigation, stakeholder management, media response.

Post Crisis Management[164]**:**

- Includes operational recovery, financial costs, market retention, business momentum, share price protection.
- Includes coronial inquests, judicial inquiries, prosecution, litigation, reputational damage, media scrutiny.

[161] *Ibid.*
[162] *Ibid.*
[163] *Ibid.*
[164] *Ibid.*

- Includes root cause analysis, management assessment, process review, implementation of change.

4.6. CRISIS MANAGEMENT APPROACHES FOR EXTERNAL ENVIRONMENT OF ORGANIZATION:

The breakdowns are not regular happenings in the organization but the result is long lasting and requires focused efforts and long lasting remedies to tackle such breakdowns. In the medium or small sized organization, the effect of external working environment based upon sector and type of such organization. The external working environment have the major effect on the technology based organization than the component manufacturing companies. This approach may be applicable and effective but it may not be important to follow all the steps as it is.

Although, the model has a focus on corrective actions rather than sudden approach in order to identify and prevent any form of crisis. For the public undertakings, the communication towards stakeholders is integral and necessary to gain the confidence in working. For private undertakings, the confidence towards internal stakeholders is more important than just to manage the crisis.

The above mentioned framework of Crisis management provides a smart and better approach, where it is to be considered for both the internal and external approaches towards crisis. This frame work is more succinct for the technology based organizations in India. The external environment[165] landscape largely based upon the clients but internal environment depends mainly on the applicable technology and the culture of organization. Issues and the crisis management relational model provides one of the most effective crises management model. This model has a focus mainly on the planning aspect of crisis management. This model implies the planning and actions which is to be taken during the pre-crisis management situation to the post-crisis management situation. It helps to create a linkage for the sufficient damage control and handles the pre and post crisis management

[165] Strategic Environmental Scanning: an Approach for Crises Management, , RESEARCHGATE , https://www.researchgate.net/publication/318699538_Strategic_Environmental_Scanning_an_Approach_for_Crises_Management (last visited Jul 24, 2020).

issues. These crisis containment models mainly provide specific methodologies and insights for a crisis management. If organizations critically examine these models they may trace and identify their potential benefits but still, there are some limitations towards the applications for medium scale and small scale organizations. These highlighted models have a prerequisite of tested and experienced work force in order to understand the crisis and effects of the crisis. These models also require separate body or team in order to manage the crisis. Although, In the medium scale and small scale organization, the employee education and awareness regarding the latest applied technologies is still a major problem.

4.7. CRISIS MANAGEMENT APPROACHES FOR INTERNAL ENVIRONMENT OF ORGANIZATION:

Crisis management approach related with internal business environment, or self-inflicted crises or the sudden unidentified breakdown in the internal systems or the system failures is much varied than the approach for the external working environment related crisis. The internal working environment[166] normally relates to the factors where the organization have direct or indirect control and these approaches can be changed or altered easily as compared to the external working environment, where organization doesn't actually have any sort of control.

The technology based organizations in India are doing consistent efforts to improve quality of the services as recently most of the companies are jumping towards remote working polices. The Information Technology industry has seen lot of change in the last 20-30 years precisely after the effective implementation of norms relating to globalization in the country which also affected the technology based organization in very much of significant manner.

Moreover, the significant contributions of quality management experts created a change in different thinking pattern about the quality of products and services. Their contribution has immensely helped all forms of technology based industries to improve

[166] *Ibid.*

service quality through continuous improvement. It has changed work culture in various countries. India really made a dramatic change to manage crisis related to process improvement, use of available resources and the services quality improvement and finally and most important, the cost effective services towards the clients to maintain their trust on them.

The contribution of Quality management experts towards the ideas of Crisis Management and approach towards containment of crisis in most effective manner, majority of their ideologies were made applicable in Japan, which is very popular for their immense technological growth and being decades ahead from various countries of the world including India, and India's organization may look forward the approaches analyzed and applied by them in their industries in order to get such a huge increment as well as smooth handling of any crisis faced by their organizations. It is really important to observe the contributions made by them in this sector which is enumerated as follows:

4.7.1. Contributions made by W. Edwards Deming[167]:

Deming has provided the two most prominent approaches for internal system process as well as product development crisis management. He proposed the PDCA cycle[168] and the Quality Philosophy. Firstly, the PDCA cycle; i.e., "Plan – Do- Check – Act" is tool of continuous improvement in order to achieve better results every time. Today, lot of variants of this cycle is used in organizations as the particular process of internal crisis management.

4.7.1.1. Guiding Principles of W. Edwards Deming[169]:

1. To create continuity of purpose towards the improvement of product and services, with the focus and target to become competitive, stay in the market and to provide adequate work and output.
2. Adopt the new ideology or philosophy.

[167] The MIT Press, *Out of the Crisis | The MIT Press*, https://mitpress.mit.edu/books/out-crisis (last visited Jul 24, 2020).

[168] PDCA Cycle - What is the Plan-Do-Check-Act Cycle? | ASQ, , https://asq.org/quality-resources/pdca-cycle (last visited Jul 24, 2020).

[169] Press, *supra* note 154.

3. To cease the dependence on inspection to achieve optimum quality. Restrict the requirement for massive audits and inspection by building quality into the services in the first place.
4. To end the practices of rewarding working on the basis of a prices.
5. To Improve consistently and forever, the technical system of production and service.
6. To Institute adequate education and training while providing professional job.
7. To Institute the quality leadership in order to help people to do a better job.
8. To remove the fear, so that everyone may work effectively for the organization.
9. To Break down the distance and barriers between the different departments of the organizations.
10. To Eliminate the sensitive slogans, exhortations and the objectives for the work force asking for the minimum defects and new levels towards organizational productivity.
11. To restrict the work standards (quotas) on the factory floor. Substitute with leadership.
12. Eliminate management by putting careful objective process. To eliminate the management by numbers and calculated goals. Instead, substitute with leadership.
13. To remove the uneven barriers that steal the hourly worker of their right relating to their pride of workmanship.
14. To remove the uneven barriers that steals the people in the management and in the engineering of their right to pride of their workmanship.
15. Institute various extensive program of the education and self-improvement.
16. To put everybody in the organization to work in order to realize the transformation. The organizational transformation is to be everybody's job.

4.7.2. Contributions made by Joseph M. Juran[170]:

[170] Joseph M. Juran, a perspective on past contributions and future impact | Request PDF, , RESEARCHGATE https://www.researchgate.net/publication/229635996_Joseph_M_Juran_a_perspective_on_past_contributions_and_future_impact (last visited Jul 24, 2020).

The main contribution made by Juran was based on the measures of quality- "Intrinsic is the belief that the quality is not incident and does not happen by accident, it must be planned". Juran also gave a powerful idea, "Quality Planning Roadmap‟.

1. To identify the right clients.
2. To determine the needs of those clients.
3. To understand those needs and provide a service that can appropriately respond to those needs.
4. To optimize the features of services so as to meet the needs of clients.
5. To develop a process which is able to produce the sufficient level of services as required.
6. To optimize the over process of the systems of organization.
7. To prove that the process can produce such provided services under the operating conditions.
8. To transfer the process towards the final operation successfully.

4.7.3. Contributions made by Philip B. Corsby[171]:

The work provided by Corsby is well known for the concepts, like 'Do it right first time' and with the 'Zero defects'. He mainly considered and emphasized on the concept of traditional quality control, acceptable quality limits, and the waiver of bad or substandard products to represent failure rather than assurance of the success.

Furthermore, Corsby has suggested exhaustive 14 steps for the purpose of overall quality improvement:

1. The commitment by the management for the overall process improvement.
2. Organization of the Quality improvement team for the purpose of process improvement.
3. Step-by-step measurement of the process improvement.
4. To make effective cost of quality and process improvement.
5. To make quality awareness as it relates to the process improvement.

[171] Philip Crosby: Contributions to The Theory of Process Improvement and Six Sigma |, , https://www.shmula.com/philip-crosby-contributions-to-the-theory-of-process-improvement-and-six-sigma/27873/ (last visited Jul 24, 2020).

6. To take the corrective actions for the purpose of process improvement.
7. Planning to implement the idea of zero defect.
8. Zero defect day effects on the process improvement.
9. The education of employees create chance for the process improvement.
10. Setting appropriate goal is important for process improvement.
11. Removal of causes for error in the process improvement.
12. Recognition of the efforts made for the process improvement.
13. Quality council for the purpose of process improvement.
14. Do it all over again for the purpose of process improvement.

4.7.4. Contribution made by Kaoru Ishikawa[172]:

Ishikawa made specific observation on the statistical methods and techniques used for the purpose of quality assessment. At the basic and simplest technical level, his contribution has mainly focused on good data collection and the presentation, for instance, use of Pareto diagram in order to prioritize the quality improvements, the cause effect structure or Ishikawa or Fishbone diagram. Ishikawa was involved in Quality Circle Movement in Japan. He also provided seven magnificent tools for the quality improvement and also provided the quality circle movement and further, the seven tools created miracles in the various organizations. The quality circle activity involved all the people at different levels and furnished a platform for every person to contribute for the improvements.

Furthermore, for effective crisis management[173], experts proposed a simpler model through interlinking the strategic management and the crisis management together. In their paper, *Anticipating and Dealing with Financial Crisis*, a simple framework is highly suggested for the organizations facing financial crisis due to any sort of disaster faced by them.

The model of crisis management provided certain steps which all are the extensions of various methodologies still in practice. The most important phase of this framework is in

[172] Kaoru Ishikawa, , SIX SIGMA STUDY GUIDE (2013), https://sixsigmastudyguide.com/ishikawa/ (last visited Jul 24, 2020).

[173] Six steps to better crisis management, http://www.beaconadvisors.us/news/articles/JICArticle.pdf (last visited Jul 23, 2020).

deciding the interlinking of each stage in crisis management with strategic management. This interlinking approach helps organizations to clearly define and form the closer relationship between crisis and any of related strategy formation to avert the prevalent crisis.

Application of strategic linkage model may vary with the perception through an individual strategist. To coping up with the crisis will surely provide the ideas for the new strategies which is to be formulated. The success of this model mainly depends upon the understanding of this approaches of crisis management as step-by-step process and through initiating a thought process at the time of taking every step, so as, how one can overcome the overall crisis and provides the long-term solutions and gives an opportunity to initiate a plan by giving it a thought for the purpose of developing strategy for curbing the crisis efficiently.

4.8. CRISIS COMMUNICATION STRATEGIES:

The failure to communicate adequately with various stakeholders during a crisis period can result to the serious consequences for an organization. The communications that carried out in an organization during a period when crisis strikes, are really critical in the phase of crises communications[174]. At the time of the crisis period, numerous response strategies have to be emerged for the organization.

There are several parts of Attribution theory also, which tends to provides a tested and useful framework for the purpose of conceptualization of the effective crisis communications management system[175] which take overs, administers and maintains that the organization's public perception or their client's perception is mainly based upon the dimensions of their locus, stability, and the controllability of the crises by the organization

[174] Robert R. Ulmer, *Effective Crisis Management through Established Stakeholder Relationships: Malden Mills as a Case Study*, MANAGEMENT COMMUNICATION QUARTERLY (2016), https://journals.sagepub.com/doi/10.1177/0893318901144003 (last visited Jul 24, 2020).

[175] DAN PYLE MILLAR & ROBERT L. HEATH, RESPONDING TO CRISIS: A RHETORICAL APPROACH TO CRISIS COMMUNICATION (2003).

and to efficiently deal with the crisis without losing the communication at that time with the stakeholders.

Understanding crises communication before, during, and after a crisis is very important in Crisis Management Plan of an organization. For instance, recently, PwC reports has stated that, the Indian organizations pursuing remote working policies should deploy the robust preventive measures in order to deal with spike in incidences of cyber-attacks following the COVID-19 outbreak in India.

Siddharth Vishwanath, Leader - Cyber Security, PwC India, stated that, with the significant shifts to work from home or the off-location operation, hackers or system breakers, who all realize this, does not want to leave any stone unturned to harness the moment. Their analysis validates this as the cyberattacks in the backdrop of the COVID-19 have seen a sudden spike towards Indian Organizations.[176]

At this stage of global pandemic, it is very crucial to realize the importance of the communication strategies towards crisis management plans as it becomes difficult to deal with such problems by the technical teams from the remote places, So, it is important for the Indian organizations to be prepared beforehand while dealing with any of such problems and to avoid the stage of crisis situations at this difficult times. Because, for some clients, protection of their personal information is very crucial and its loss may even lead to the setback of country's economy.

The current trends in crisis management have faced a paradigm shift from the employee excellence to the technological excellence. Today, organizations deal about employee as an asset and organizations are giving more emphasis on the technological development as per changing times. There is shift from human resource to the technology. Today, efforts are made by various organizations in order to explore the highest technological potential and organizations have changed their approach from the skill development to technical-development. These new trends may not be currently clearly being observed in the medium and small scale organizations because of the limitation of their infrastructure. These organizations have limitations in business and thus, they equip

[176] *Siddharth Vishwanath*, PwC , https://www.pwc.com/us/en/contacts/s/siddharth-vishwanath.html (last visited Jul 24, 2020).

the best possible technologies to reduce the recurring human expenses. These organizations also do agree the importance of these technological shift which tends to not only saves money but also time of the organizations as well as of their clients while getting the required output.

In order to sum-up this chapter, the human efforts combined with the positive technological development may manage crisis in better way if properly understood and managed each individual phases in an above mentioned defined process. Unfortunately, in many instances, management still takes only a reactive position, viewing crisis management activities mostly as a means to the activities of coming back as soon as possible to the business as usual. Planning in advanced is the only way that the responsible organizations in order to win over the challenges over this potential crisis.

By proper crisis planning and crisis training in advance, the adverse effects of a crisis on the organization, and on the stakeholders, can be significantly reduced, and the opportunities that a crisis serves can, at the same time, be enjoyed and utilized efficiently by all directly or indirectly related to the technical and operating functions of the organization.

The upcoming chapter introduces the second phase of the study, which is related to the problems of cybercrimes which is faced by the organizations of India. It includes the concepts, ideas, meanings, measures, legal prospects and judicial approaches in Indian courts towards cybercrimes in India.

It also includes various important case laws in order to understand these crimes in detailed manner with the Indian perspective in order to curb this menace in the future especially with the focus on technology based organizations in India.

CHAPTER 5

CYBER CRIMES IN INDIA: MEANING, SCOPE AND HISTORICAL ASPECTS

"One of the main Cyber-risks is to think they don't exist.
The other is to try to treat it's all potential risks."

- Stephane Nappo
Global CISO

The new technology has become very imminent factor for almost every sectors and it is also shaping a new generation of crimes which has been cropped by the advent of internet attacks, software piracy, Internet pedophilia, E-espionage, breaking password, email bombings, spoofing, frauds telecommunication, frauds, pornography and the circulation of the illicit or the unlicensed products and services are the offences that have already made their signs. There are new problems emerging related with it such as credit card fraud, cyber terrorism, cyber laundering and the unauthorized use of secure Internet communications.

The present weak electronic payment system without having any adequate safeguards is posing a serious risk of an unauthorized withdrawal from banks and the counter money laundering operations through the internet. Software piracy is a boom in the business and phonographic organizations are sinking day by day across the world.

5.1. CONCEPTS AND CLASSIFICATION OF CYBER CRIME:

With the step-by-step evolution of the human brain, the modes of committing crime are also changing drastically. The criminals are even getting smarter day by day and are using their minds in this context to commit crime with clean surface and escape without getting caught. With the advent of technology, no one thought that it will become a made or major source of committing crimes.

The term cybercrime[177] is manipulatively applied name. This term has nowhere been defined in almost any related statute/ Act passed or enacted by the Parliament of India.

[177] cybercrime | Definition, Statistics, & Examples, , ENCYCLOPEDIA BRITANNICA , https://www.britannica.com/topic/cybercrime (last visited Jul 24, 2020).

The concept of cybercrime is not radically varied from the concept relating to the conventional crime. They both include the conduct whether act or omission which leads to breach of rules of law and are counter balanced through the sanctions of the state. Though, the cybercrimes are a new breed of crimes which came into being right after the advent of the internet and the scenario has become even worse with the influence of dark internet in the society.

5.1.1. Conventional Crime:

Crime is to be considered as a social, political and economic phenomenon and is as traditional as the human society. Crime is an ethical and legal concept and has the selection of the Law. The Crime or an offence is a legal wrong which can be followed by the appropriate criminal proceedings which may result into the punishment. The basic sign of any criminality is that it is breach of the criminal law, according to Lord Atkin, the criminal level of an act cannot be discovered through reference to any standard but one is the act prohibited with the penal consequences. A crime can have said to be any conduct followed by act or omission prohibited by the law and consequential damage of which is visited by the penal consequences.[178]

5.1.2. The term Cybercrime:

Cybercrime is the latest and perhaps the most complicated problem in the cyber world. Cybercrime may be said to be those species of which genus is the conventional crime and where either the computer is an object or subject of the conduct constituting crime. Any criminal activity that uses a computer either as an instrumentality target or means for perpetuating further crime comes with in the ambit of cybercrime.[179]

A generalized definition adopted to define the term cybercrime may be “Unlawful acts where in the computer is either a tool or target or both.” The Computer may be used as a weapon for the following kinds of activities such as financial crimes sale of illegal articles, pornography, online gambling, online intellectual property crime, E-Mail Spoofing, forgery, cyber defamation, cyber stalking. The computer may also however be a

[178] CONVENTIONAL CRIMES are traditional, illegal behaviors, , http://sociologyindex.com/conventional_crime.htm (last visited Jul 24, 2020).

[179] cybercrime | Definition, Statistics, & Examples, *supra* note 164.

target for various unlawful acts in the various cases i.e., unauthorized access of the computer data, computer programs/computer networks, theft of important information retrieved in the electronic form, e-mail bombing, various salami attacks, logic bombs, Trojan attacks, Internet time thefts, Web jacking, Theft of the computer system, any physically damaging of the organization’s computer system containing important information.

5.1.3. Difference between Conventional Crime and Cyber Crime:

Apparently, there is no per se distinction between cyber and conventional crime as both the crimes amounts in to some sort of loss to any of the parties. However, through a deep introspection, it can be said that, there is a fine line of the demarcation between the conventional crime and the cybercrime which may be appreciable. The main demarcation is visible in the way of involvement of the medium in the cases of cybercrime.

So, Cyber Crimes can also be defined as, Crime committed against the Individual or Organization by any means of Computer is to be called as Cyber Crime. Cybercrimes are those forms of crimes which are committed on a network environment or through an internet.[180]

5.1.4. Identification of Cyber Criminals:

It can be identified as, any person who tends to commits or commits an illegal act with an intention of guilty or commits any crime is called an offender or a criminal. With this context, any person who commits a cybercrime may also be known as a cybercriminal. The cyber criminals may be a children and an adolescent aged below 6-18 years, they can be an organized hacker or may be professional hackers or crackers, also discontented employees, cheaters or even any psychic persons.[181]

[180] Distinction Between Conventional And Cyber Crime Information Technology Essay, , https://www.ukessays.com/essays/information-technology/distinction-between-conventional-and-cyber-crime-information-technology-essay.php (last visited Jul 24, 2020).

[181] How to identify and stop a cybercriminal, , THE ECONOMIC TIMES , https://economictimes.indiatimes.com/tech-life/how-to-identify-and-stop-a-cyber-criminal/slideshow/47081619.cms (last visited Jul 24, 2020).

5.2. REASONS FOR CYBER CRIME:

The famous scholar Professor H.L.A. Hart in his classic work titled "The concept of Law"[182] has stated that human beings are vulnerable to unlawful acts which are called as crimes and therefore, the rule of law is required to protect them against any such acts. By applying the similar analogy towards cyber space, the technology systems despite being the hi-tech devices, are highly vulnerable. This technology can easily be applied to exploit any person or his computer through illegal or unauthorized access. The crisis so caused to the victim may be the consequences of the abuse of technology systems. In the absence of any full-fledged mechanism to protect or safeguard the intermediate computer users against such cyber criminality, the cyber criminals may indulge in such criminal activities through the networks which is unabated without any fear of being apprehended and to be applied for the offence committed by them. The main reasons for such vulnerability of computers to cyber criminality[183] may briefly discussed as follows -

1. Huge Data Storage Capacity:

The computer has the important characteristic of capacity of storing the huge data in a comparatively small space. A single small microprocessor chip can store lakhs of pages in the CD-ROM. This storage capacity has enough space to collect or derive the information either through physical or through visual medium in much simpler way. Any data stored in ROM remains intact even if the power is breached or turned off. Whatsoever be the form of ROM used, the data stored therein is to be non-volatile and will remains there indefinitely until and unless it is intentionally removed or over written.[184]

2. Wider Access to the Information:

The dissemination of the information through world wide web has created new resources for the speedier and cost effective easy access to the information throughout the world. It has also created the new environment of emails, social networks, downloads etc. Today, each and every one can be reached just a mouse click away from another. However,

[182] H. L. A. HART, HERBERT LIONEL ADOLPHUS HART & LESLIE GREEN, THE CONCEPT OF LAW (2012).

[183] Cyber Crime, Computer's Vulnerability, , http://cybercrime.planetindia.net/computer_vulnerability.htm (last visited Jul 24, 2020).

[184] *Ibid.*

the wider access of the information leads to some problems like the protecting and preventing any network system against an unauthorized access where there is possibility of information breach, not due to some human error, but due to the complex technical manipulations. For instance, the bank vault which mainly contain jewelry, lakhs of rupees are well guarded against such unauthorized access by the miscreants as it may be made up of very strong materials located in a reinforced room strictly guarded by the security personal. The trusted officials of the bank reserve the password keys and/or any other access code secret. But despite with all these security measures, the bank's servers which can virtually control hundreds of arrears of rupees are far easier to break through cracking the strongest core firewalls and even the biometric authentication system. A secret pattern can be easily breached and stolen by applying the logic bombs or the key images to the access codes. Similarly, the high-level voice recorders can easily fool voice lock systems and can breakdown all the security measures.[185]

3. Negligence by Network Operators or Users:

The errors are closely related to the human conduct. It is, thus, more probable that while securing and protecting the network systems, there might be any lapse or loophole done by the owner/user which may emerge as an opportunity for the cybercriminal to gain the unauthorized or illegal access over such networks. The interaction with the cross-section of certain computer users has also shown that in their anxiety to put the computer software into the continuous operation, they allow such access, control and security measures by taking a back seat, thus, providing such scope for the cybercriminals to intrude and to steal, alter or remove the substantial data. This can be specifically affirmed with the big organizations such as the banks, corporations Government offices etc. which are nicely equipped with the high-level software systems towards public access but sometimes leave it totally insecure and unguarded against information breakers or manipulators due to the sheer negligence of any staff or any employees.[186]

4. No availability of lost evidence:

[185] *Ibid.*

[186] *Ibid.*

The traditional approaches for producing, storing, transmitting and dissemination information or any records has now been replaced by the current digital processing and the network technology. The Real problem comes before the law enforcement and for the investigating agencies is how to procure and preserve such evidence in potential form. Unlike, the traditional offences, it is very hard to collect and preserve the sufficient evidence of a cybercrime which could with the stand to establish the guilt of the cyber accused beyond any reasonable doubt. internet provides the anonymity to the cyber criminals which encourages them to indulge in the criminal activity without leaving any potential evidence and even if some evidence is left, it is rarely sufficient to convince the police that a criminal case is to be registered against such perpetrator. The miserably low rate of cybercrimes conviction is a highlight to the fact that most cyber criminals erase or destroy the evidence in order to escape through the conviction.[187]

The inadequacy of such traditional approaches of collecting evidence and crime investigation has now necessitated the adoption of new approach can be termed as techno-legal procedure now called cyber forensics, which has widely been classified as the computer forensics and also network forensics.

5. Jurisdictional Problems:

Cybercrimes roams across the territorial borders which undermine the feasibility and legitimacy of applying the domestic procedural laws which are normally based on the geographical locations or the territorial jurisdiction, cybercrimes are committed mainly through the interconnectivity of cyber space network and thus, they do not recognize any geographical limitations because of they are mainly transnational in nature. There being no any uniformity in law and procedure among the different countries for handling such cases of cyber criminals, the Jurisdictional conflict creates a serious threat towards any nation to deal with the cyber offenders effectively. In many cases, it may happen that a particular cyber activity can be recognized as a crime in one country but it is not so in the other country under which the criminal or the victim resides, as a result, the criminal almost always easily escapes prosecution. In the absence of any uniform internationally

[187] *Ibid.*

recognized code of law and procedure governing the cybercrimes, the law enforcement authorities of the individual countries find it extremely impossible to tackle the cybercrimes and crimes which applying their territorial law. In brief, it is stated, reporting and conviction rate in cyber cases is very far & few due to the paucity of cyber law jurisdiction of the country investigating or trying such offences and this uncertainty of law encourages the cyber criminals more to enhance their nefarious activities unabated.[188]

5.3. MODES AND WAYS OF COMMITTING CYBER CRIMES:

Cybercrime may be committed by just a mere mouse click and without the knowledge of the victim, thus, leaving the victim totally incapacitated. In various cases, the victim even does not know that he or she has been subjected to a serious cybercrime and eventually became a victim of it.[189]

1. Hacking:

There are various kinds of offences which all are normally referred as hacking in the generic sense. However, the creators of the information technology Act 2000 have not used this term in order to avoid any form of confusion, people would not interchangeably use the word hacking for the purpose of unauthorized access as the latter has even wide connotation.

Traditionally, the term 'Computer hacking' describes the penetration of the computer system which is not carried out with the aims of manipulation, sabotage or espionage, but only for the satisfaction of overcoming the technical security measures.

Hacking may be operated just for the sake of challenge or as an adventure, in order to do unlawful activities or due to the habit. Hacking can be done mainly by the way of two types i.e. against computer and against the network.[190]

[188] *Ibid.*

[189] Mode And Manners Of Committing Cyber Crime, Information Technology, https://www.ukessays.com/essays/information-technology/mode-and-manners-of-committing-cyber-crime-information-technology-essay.php (last visited Jul 25, 2020).

[190] Hacking and cybercrime, , RESEARCHGATE , https://www.researchgate.net/publication/228705030_Hacking_and_cybercrime (last visited Jul 25, 2020).

2. **Theft of electronic information:**

This includes informations stored in the computer hard disks system, the removable storage media etc. Theft may be either by misappropriating the data physically or by tampering them through any virtual medium.[191]

3. **Email Bombing:**

E-mail bombing also refers to the sending a large amount of e-mails to the victim leading in the victim's e-mail account (in case of an individual) or to the servers (in case of company or an e-mail service provider) breakdown. An easier way of achieving this would be subscribing the victim's e-mail address to reasonably a large number of mailing box lists. Mailing box lists are the different interest groups that may share information on a common cybercrime and the related laws in India with one another via e-mail. Mailing box lists are very famous and may create a lot of daily e-mail traffic based upon the mailing list. Some of them creates only few messages per day, while the others create hundreds of such types of messages. If a person has just unknowingly or by mistake subscribed to hundreds of mailing box lists his incoming e-mail traffic will be too large and his service provider may probably delete his account.[192]

4. **Salami Attacks:**

This kind of crime is normally happened towards the financial institutions or for the purpose of committing the financial related crimes. An important characteristic of this form of offence is that the changes is so small that it would normally go unnoticed.[193]

5. **Worms or Virus Attacks:**

Viruses are the programs that get attach themselves to a computer or a file once get inside and then circulate themselves towards other files and towards other computers connected on a network. They usually affect the data saved on a computer either by altering

[191] Cyber Theft – A Serious Concern In India - Criminal Law - India, , https://www.mondaq.com/india/white-collar-crime-anti-corruption-fraud/785836/cyber-theft-a-serious-concern-in-india (last visited Jul 25, 2020).

[192] MS-ISAC Security Primer - Email Bombs, , CIS , https://www.cisecurity.org/white-papers/ms-isac-security-primer-email-bombs/ (last visited Jul 25, 2020).

[193] Aj Maurya, *what is a Salami Attack*, AJ MAURYA. AN ENGINEER. (2014), https://ajmaurya.wordpress.com/2014/03/27/what-is-a-salami-attack/ (last visited Jul 25, 2020).

or by deleting it. Worms unlike virus do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.[194]

6. Trojan Attacks:

This term has its origin from the word, Trojan Horse, is a harmless and friendly looking program which causes erosion and loss, when get activated. Its deceptive look is its primary phase and can notation where by it cannot be traced or controlled, until the damage is finally done. It is mainly used as a camouflage for the malignant designs of the perpetrators. Its attack of surreptitious nature makes it very difficult to enter or control it at the right moment. It is created as something as benign such as a directory lister, archiver or game or even a program to find and destroy viruses. It is also used to capture the passwords of the legitimate users or clients of the system which is done by impersonating the normal system log in program. A special case which is to be referred of Trojan Horse is the Mockingbird software that intercepts communications, mainly, login transactions between the users and the hosts and provides exact system-like responses to the users while saving their responses in the background for instance, account IDs and passwords.[195]

7. Internet Time Thefts:

Normally in these kinds of thefts, the Internet surfing hours of the victim are used up by the another person. This is done by appropriating the access to the login ID and the password of another person.

Internet time theft is an offence when some unauthorized person robes the hours of the Internet to be used by any other person. Generally, internet is a kind of pay-off service i.e., in order to avail the internet services, a person needs to pay the money to the ‘Service Provider’ at a particular duration. For instance, the colonel Bajwa's case- the Internet hours were used up by some other person. This was, perhaps, one of the first reported cases

[194] What is a computer worm and how does it work?, , https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html (last visited Jul 25, 2020).

[195] What is a Trojan Virus?, , WWW.KASPERSKY.CO.IN (2019), https://www.kaspersky.co.in/resource-center/threats/trojans (last visited Jul 25, 2020).

relating to the cybercrime in India. However, this case made the police infamous so as to their lack of awareness and understanding of the nature of such cybercrime.[196]

8. **Web Jacking:**

This term is derived from the term ‘hi jacking’. In these kinds of offences, the system breaker or hacker appropriates access and control over the website of another person. That may even multiplicative or change in the information on the site. This may be done for the purpose of fulfilling any political objectives to gain the money. For instance, the “Gold fish” case. In this case, the site was hacked and the Information pertaining to gold fish was taken and changed. Further, a ransom of almost 1 million US $ was demanded as the ransom. Thus, web jacking is a process whereby control over the site of another is hacked to get some consideration for it.[197]

5.4. THE CLASSIFICATION OF CYBER CRIME:

With the expanding dimensions of cybercrime in India, it became necessary to analyze as to how these crimes vary from others in nature and in its form. Therefore, varied actions which may amount to crime and comes under the criminal related activities have been broadly classified into three main categories as follows:

1. **Cyber Attack where the Computer is used as a target[198].**

In this category of cybercrimes, computer is itself a target for the crime. The crimes which are covered under this category can be classified as-

i) Sabotage of computer systems or computer networks.
ii) Sabotage as operating systems and programs.
iii) Theft of data or information.
iv) Theft of intellectual property such as computer software.

[196] Cyber frauds in India, , https://www.indiaforensic.com/compcrime1.htm (last visited Jul 25, 2020).
[197] What is web-jacking? | Karnika Seth - Cyberlawyer & Expert, , https://www.karnikaseth.com/what-is-web-jacking.html (last visited Jul 25, 2020).
[198] Cyber Crime - Computers As Targets Or Criminal Tools, , https://law.jrank.org/pages/11983/Cyber-Crime-Computers-targets-or-criminal-tools.html (last visited Jul 25, 2020).

v) Blackmailing based on information gained from computerized filed such as personal history sexual preferences, financial data etc.

vi) Theft or marketing information.

2. **Cyber Attack where the Computer is an instrument facilitating any related crime**[199]:

The development of micro-computers has generated new versions of traditional crimes, for example, software piracy, copyright violation of computer programs, theft of technological equipment is covered under this category of crime. Illegal sale of duplicate database is yet another example of this type of cyber space crime.

3. **Cyber Attack where the Computer is incidental to such committed crime**[200];

Forms of crimes included in this category are those in which the computer system is not essential for the crime to occur, but any sort of computerization does help in the incidence of crime by processing of large number of information and makes this crime more difficult to get traced and identified. The best illustration of this species of crime is, the cases of money laundering and illegal banking transactions. In one of the case, a suspect committed murder by changing a patient's medical prescription and dosage in a computer of the hospital.

In various cases, the cyber criminals even damage the storage media such as disks in order to clearly destroy evidence relating to their crime.

5.4.1. Traditional Classification:

[199] *Ibid.*

[200] *Ibid.*

The cybercrimes[201] which includes two different group of such crimes, namely:

1. **Economic related Cybercrimes:**

In some of the cybercrimes of economic type, the computer technological system generally software as well as the hardware, is the target for the criminal activity. Some of such crimes are below mentioned as follows:

a) Fraud committed by manipulating the systems of computer. i.e. the perpetrator of the crime manipulates the data contained in the computer system for the illegal gains.
b) Illegal copy of the software and computer database to procure information for criminal purposes.
c) Sabotage which causes damage to the computer system comprising hardware as well as intangible elements contained in computer program.
d) Illegal use of computer systems belonging to other person without authorization.

The economic cybercrimes involve intrusion in computer systems without authorization, with the fraudulent purpose of sabotaging or causing damage. The offender in these crimes surpasses the access barriers for accomplishing his ulterior motives at the cost of victim agony.[202]

2. **Cybercrimes against Privacy:**

In cybercrimes involving violation of right to privacy, the computer system is used as a tool for perpetrating the criminal act. Truly speaking, several behaviors stated above as cybercrimes of economic type are similar to those that would correspond to this category of cybercrime, the only difference being that the behavior would not affect any proprietary right of the victim, instead would affect his legal right such as right to privacy.

Ordinarily, the term privacy means one's right to be left alone. But with reference to internet transactions, it consists anonymity, that is, a person's identity and information

[201] Ulrich Sieber, *International cooperation against terrorist use of the internet*, Vol. 77 REVUE INTERNATIONALE DE DROIT PENAL 395–449 (2006), https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-395.htm (last visited Jul 25, 2020).
[202] *Ibid.*

about him should not be disclosed. Thus when a person provides information to a bank, merchant, doctor or a lawyer, he expects that the said information should be used solely for the purpose for which it is meant and not be disclosed to other's without that person's express or implied consent. But there are instances when online secret or personal information received from the clients is disclosed by unscrupulous persons for ulterior purposes, well beyond the purpose for which it was given. Similarly, when a person sends an e-mail message, he expects that it will be used only by the intended recipient and no one else. But unfortunately this right of privacy remains largely unprotected and may be used for furtherance of a criminal activity. In case of other secret and confidential records stored in computer, the confidentiality and secrecy thereof has to be protected in exercise of user's right to privacy so as to prevent it from being misused by cyber criminals.[203]

5.4.2. The General Classification:

Although, the classification of cybercrimes into economic type or privacy mainly affecting behavior as also the manner in which they are committed by the help of computer as a main target, or also as an instrument helping such commission of crime has been highly endorsed by most of the authorities, but general classification comprising three categories[204] namely 1) Cybercrime against persons 2) Cybercrimes against all forms of property, and the 3) Cybercrimes against society as a whole or the state sounds to be most rational and logical.

1. **Cybercrime against persons:**

These crimes are committed against individual persons by disturbing him either physically or mentally. Such offences include various forms of crimes such as the transmission of child pornography harassment operated with the use of systems or e-mail threats or cyber stalking, dissemination of any obscene, indecent or defamatory material etc.[205]

[203] *Ibid.*

[204] Cyber Crime: Types, Examples, and What Your Business Can Do, , EXABEAM (2019), https://www.exabeam.com/information-security/cyber-crime/ (last visited Jul 25, 2020).

[205] Cyber Crime – A Threat to Persons, Property, Government and Societies by Shital Kharat :: SSRN, , https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2913438 (last visited Jul 25, 2020).

2. Cybercrimes against various forms of properties:

These crimes are mainly committed to affect the property of a person through any electronic medium causing damage or loss to such person. These include an unauthorized computer intrusion for the purpose of cyber space computer vandalism and the transmission of dangerous programs and the illegal possession of computerized information etc.[206]

3. Cybercrimes against the society or State:

The Cyber terrorism is one distinct form of criminal activity falling under this category. The enhancement of internet has shown that the medium of cyberspace is being more misused by the individuals and the groups to threaten the government officials and also in order to terrorize the citizens of country. These crimes mainly manifest itself into terrorism, where an individual crack into a website maintained by the Government official or its Defence Department.[207]

These crimes also include the trafficking financial crimes such as sale of illegal articles, online gambling etc. All the aforesaid categories of cybercrime clearly indicate that the growth of information and communication technology has created a variety of crime which were hitherto unknown to the human society till now. These crimes may further have briefly discussed under the following heads-

I. Cybercrimes against Persons:

Cyber offenders make use of computer, systems and networks for the purpose of committing offences against person or individual. The online offences which may be committed against organization/individual may be stated as follows:

a) Harassment through e-mails:

Cyber harassment is a distinct form of crime. There are various forms of harassment which may and do occur in the cyber space or by any mode which takes the use of cyber space. Harassment through e-mails now a day is a common phenomenon. It is

[206] *Ibid.*
[207] *Ibid.*

resembling to harassing through letters. Harassment may be sexual racial, religious or in any other form. Cyber harassment is a crime which relates to violation of privacy of citizens which indeed is a serious crime. No one likes that any random person should invade his/her invaluable right of privacy, which the medium of internet grants now to almost every person.[208]

b) Cyber Stalking:

Cyberstalking mostly occurs with women who are stalked by the adult pedophiles. A cyber stalker does not have to leave his home in order to directly stalk his or her target and has no fear of physical avenge since he knows that he cannot be physically felt in the cyberspace. He may be altogether on the different side of the earth or may be a neighbor or even a relative and they could be of either sex. Cyber stalking is also regarded as the Cyber Teasing. The person who via e-mail or certain messages which are in electronic form tries to accuse any person or defames his reputation in society is said to be a cyber-stalker.[209]

c) Disseminating the Indecent Material/ Pornography or pal-luting from obscene exposure:

The term "dissemination of Indecent material" is a very broad term which includes the sale, distribution, exhibition and promotion of a material which is indecent by the use of the technology. A material is said to be obscene, when it predominantly puts an average person into the contemporary community towards a shameful or morbid interest in nudity, sex or excretion, or such material, if taken as a whole lacks serious literary, artistic, political or scientific value.[210]

Pornography can be defined as the explicit presentation of any sexual activities virtually or descriptively to become erotic rather than aesthetic feelings, films literature etc. According to the Collin's dictionary, the word pornography implies the writing films or pictures designed to be sexually exciting.

[208] Canadian Centre for Occupational Health and Safety Government of Canada, *Internet Harassment or Cyberbullying : OSH Answers* (2020), https://www.ccohs.ca/ (last visited Jul 25, 2020).
[209] *Ibid.*
[210] *Ibid.*

These obscene materials may pervert the minds of the adolescents and lead to deprive or corrupt their mind. Section 67 of the IT Act, describes that "a person who publishes or transmits or causes to be published in the electronic form, any material which is lascivious, or if its effect is such as to tend to deprave and corrupt person who are likely to read, see or hear the matter contained or embodied in it, is liable to be punished on first conviction with imprisonment up to three years and with fine which may extend to rupees five lakh and in the event of a second or subsequent conviction, with imprisonment up to three years and with fine, which may extend to rupees lakh and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine, which may extend to ten lakh rupees."[211]

The important elements of such offences are publication and transmission through any medium, of pornographic material, in any electronic form.

Two well-known cases relating to pornography that may be important to note at this juncture are Delhi Bal Bharti Case and Bombay Swiss Couple Case.

In the *Air Force Bal Bharti School & Anr. V. Delhi School Tribunal & Ors. (LPA No. 48 of 2005)*[212], also known as Delhi Case, "a school student was teased by all his classmates for him having a pockmarked face. Fed up with cruel jokes, he decided to get back at his tormentors and set up a website with pornographic material and scanned photographs of his classmates and teachers morphed them with nude photographs and put them upon website that he uploaded on a free webhosting service. It was only after the father of one of the class-girls featured on the website objected and lodged a complaint with the Delhi Police that an action be taken against such offender.

The counsel representing the girl's parents who had filed the complaint said that there would be no compromise on the issue and the boy accused of setting up the website with pornographic material must be rusticated from the school. He claimed that there were

[211] Section 67 of Information Technology Act: Punishment for publishing or transmitting obscene material in electronic form, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-67-punishment-for-publishing-or-transmitting-obscene-material-in-electronic-form/ (last visited Jul 25, 2020).

[212] Air Force Bal Bharti School & Another Vs. Delhi School Tribunal & Others, , HTTPS://WWW.LEGITQUEST.COM , https://www.legitquest.com/case/air-force-bal-bharti-school-another-v-delhi-school-tribunal-others/7f2f6 (last visited Jul 25, 2020).

other twelve children of the school whose names were mentioned in the website and the parents of these children wanted the expulsion of the accused from the school as they did not want their children to study with him.

The father of the accused boy had brought some evidence that even before his son had set up the pornographic website, other students had been sending objectionable e-mails about the teacher's and the principal of the school. But the complainant alleged that the material had been presented by the father of the accused boy only to divert the attention of the court. He pleaded that contents of the website amounted to character assassination, whereas the said e-mails were much milder. However, after a great deal of persuasion by the court, the case was compromised by the parties."

In the *Bombay Swiss Couple Case*[213], "Swiss couple used to gather slum children and then force them to appear for obscene photographs. They would then upload these photographs to websites specially designed for pedophiles. The Mumbai police arrested the Swiss-Couple for pornography and they were convicted for the offence under section 67 of the Information Technology Act[214] read with Section 292 of Indian Penal Code[215]."

Child Pornography:

Child Pornography itself constitutes a separate category of a cybercrime. This offence is committed by the use of technology and the internet by its abusers to reach and abuse children sexually throughout the world at any place. The constant use of this technology has made the children a vulnerable victim of this Cyber Crime.

d) Defamation:

Defamation is an act of imputing the reputation of any person with intent to be lowering him in the eyes of the right thinking members of the society, mainly to cause him to be shunned or avoided or to expose him towards hatred, contempt or to ridicule. Cyber

[213] TNN | Mar 29, 2003 & 23:57 Ist, *Swiss couple gets 7-year term in child porn case | Mumbai News - Times of India*, THE TIMES OF INDIA , https://timesofindia.indiatimes.com/city/mumbai/Swiss-couple-gets-7-year-term-in-child-porn-case/articleshow/41800896.cms (last visited Jul 25, 2020).

[214] Section 67 of Information Technology Act, *supra* note 198.

[215] The law of obscenity under Section 292 of the Indian Penal Code, 1860 – The Chambers of Law, New Delhi, , https://www.tclindia.in/the-law-of-obscenity-under-section-292-of-the-indian-penal-code-1860/ (last visited Jul 25, 2020).

defamation is not different from the adversarial concept of defamation except the involvement of cyberspace medium in it.[216]

e) Unwanted Access:

As mentioned under Section 2(1)(a) of the Information Technology Act[217], the word “Access” means the entry into or instructing or communicating with the logical, arithmetical, or memory function resources of a computer system or computer network. Unauthorized access would, therefore, mean any kind of access without the permission or authorization of either the rightful owner or the person in charge of a computer, computer system or computer network.

“Unauthorized access”, according to the Information Technology Act, 2000 reads as follows: “Whoever, with the intention to cause or knowing that he or she is likely to cause wrongful loss or damage to any other person, destroys or removes or alters any information available in a computer resource or reduces its value or utility or affects, it injuriously, by any means is said to commit cracking or hacking through the unauthorized access.”[218]

f) E-mail related Cybercrimes:

In recent time, e-mail is the world's most commonly used form of communication. It is a form of communication which makes the message to cover a long distance throughout the world. However, like other means of communication. It is also being heavily misused for personal gains and ulterior purposes. The easiness, speed and relative anonymity of e-mail have been made it a powerful tool for criminals to commit cybercrimes. It is the most frequently used media of crime by the criminals for the accomplishment of their criminal motives.[219]

[216] Subodh Asthana, *Cyber Defamation in India: Laws and Challenges*, IPLEADERS (2019), https://blog.ipleaders.in/cyber-defamation-india-issues/ (last visited Jul 25, 2020).
[217] Secton 2: Definitions, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/secton-2-definitions/ (last visited Jul 25, 2020).
[218] Privacy and the Information Technology Act — Do we have the Safeguards for Electronic Privacy? — The Centre for Internet and Society, , https://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy (last visited Jul 25, 2020).
[219] E-mail related crimes, , http://cybercrime.planetindia.net/email_crimes.htm (last visited Jul 25, 2020).

II. Cybercrimes against Properties:

Systems may also be being used as an effective media or an instrument for the purpose of committing crimes relating to property. Some of these cybercrimes may be as follows:

1. Computer System Vandalism:

Vandalism, in its literal sense, means the deliberately destroying or damaging the property of any other. Thus, the concept of computer vandalism covers within it, any sort of physical damage or harm done towards the computer of any other person. These acts may take the shape of misappropriation of a computer or any related body, some part of a system or the peripheral attached with the computer or through physically breaking any computer or its peripherals. The intention of the offender behind it is generally to cause damage or harassment to such system owner.

The use of technical programs or internet to hinder the normal functioning of a computer system through the intrusion of viruses, warms or logic bombs is also referred to as the computer sabotage, where, the cyber criminals use it to gain wrongful economic advantages over a rival competitor or in order to promote the rival illegal activities of terrorism, or to steal the data of related programs for the misappropriation of money.[220]

2. Denial of Service (DoS) Attacks:

Denial of service attack (DoS) is a malicious attack which denies the users legitimate access to a computer resource. It may be in any of the following forms:

a) Attack which damage or completely destroys the resources.
b) Attack which causes the computer system to go down;
c) Attack which causes access to a computer system to be withheld from its legitimate user;

[220] Computer Vandalism, , WWW.KASPERSKY.CO.IN (2017), https://www.kaspersky.co.in/resource-center/threats/computer-vandalism (last visited Jul 25, 2020).

d) Attack which forces a processing (input or output) system to slow down or stop completely. The most common form of this attack is internet worm or e-mail bombing or spamming.

Under the Denial of service attack (DoS) the computer of the victim (sufferer) is swamped with more request than it can handle there by causing the resource (e.g. a web-server) to crash, denying authorised users the service offered by such resource. These attacks are usually launched to make a particular service unavailable to someone who is authorised to use it. This can be launched either by using one single computer or computers across the world, where there are many computers in the source for launching it is known as 'distributed denial of service attack' (DDoS).[221]

3. Intellectual Property Crimes:

Intellectual property consists of a bundle of rights. The common forms of intellectual property rights violations are software piracy copyright infringement, trade-mark and service mark violations theft of computer source code etc. The internet is a fast developing telecommunication and information system. It has become one of the most favored and convenient media to conduct business. Such efficient telecommunication and information system has to conduct business. Such efficient tele-communication and information system has strengthened legitimate commercial activities in the present day fast paced global market which may also be easily used by the criminal networks. The explosion of digitization and the internet have further enabled intellectual property violators to easily copy and illegally distribute trade secrets, trade-marks logos etc.[222]

The courts in India, have decided several cases regarding violation of intellectual property rights on the internet. Thus, is *yahoo Inc. V. Akash Arora*[223], the Delhi High Court granted relief to the petitioner yahoo Inc. who sought injunction against the defendants for attempting to use the domain name "Yahooindia.com" for internet related services.

[221] What is a denial of service attack (DoS) ?, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos (last visited Jul 25, 2020).

[222] Cyber Crime - Intellectual Property Theft, , https://law.jrank.org/pages/11992/Cyber-Crime-Intellectual-property-theft.html (last visited Jul 25, 2020).

[223] Yahoo! Inc. v. Akash Arora and another, 1999 Arb. L. R. 620, , BANANAIP COUNSELS (2018), https://www.bananaip.com/ip-news-center/yahoo-inc-akash-arora/ (last visited Jul 25, 2020).

yahoo.Inc. who were the owners of the trademark “YAHOO” and also the domain name "yahoo.com" contended that by adopting deceptively the similar domain name, the defendants were trying to cause confusion by copying the format, contents, lay-out etc. of the plaintiff's prior created regional section on their website. The defendants, on the other hand, contended that the provisions of the trademark act were not attracted in this case. This Court however, ruled in favour of the plaintiff and held that although service marks are not recognized in India, the services rendered are to be recognized for “passing-off” actions.

In yet another case of *Rediff communication limited V. Cyber booth and Ramesh Nahata*[224], the Bombay High Court held that a domain name is more than an internet address and is therefor, entitled to protection under the Trade Marks Act[225].

4. **Theft of Data and Data Diddling:**

Data theft is perhaps the most unique crime which the cyber criminals commit by breaking into a system and steal sensitive data or information and leave to return the same after accomplishing the purpose for which it was stolen. If the person affected by such theft is not vigilant in safeguarding the system against such data thefts, he will never know that such theft has occurred. It is for this reason that data-theft remains unnoticed in most of the cases. Data diddling is a simple and common computer related crime which involves changing data prior to or during input into computer. Data can be changed by anyone involved in the process of creating recording, encoding, examining, checking converting or transporting computer data. This crime can be minimized by applying internal security control measures.[226]

III. **Cybercrimes against Society or State:**

[224] Intellectual Property in the Internet Age-Ppt. | Trademark Dilution | Intellectual Property, , SCRIBD , https://www.scribd.com/presentation/217066562/Intellectual-Property-in-the-Internet-Age-Ppt-ks-Doc-1 (last visited Jul 25, 2020).

[225] ClearTax, *Trademark Act, 1999*, https://cleartax.in/s/trademark-act-1999 (last visited Jul 30, 2020).

[226] Data Alteration or Diddling, , DIGITAL FORENSICS (4N6) (2016), https://www.digital4n6journal.com/data-alteration-or-diddling/ (last visited Jul 25, 2020).

There are certain cybercrimes which seriously hamper the safety and security systems of the state and several times have the devastating effects on the whole society. One among these crimes is terrorism or terrorist activities carried out by extremist groups against the government organizations.

1. **Cyber terrorism activity against Country or Government:**

The term cyber terrorism may be defined as 'any person, group or any form of association who, with the terroristic intentions, utilizes, refers or cause to access a system or computer network or any electronic system or device or by any available means and thereby intentionally involves in or attempts to engage in any form of terrorist act, commits the offence of cyber terrorism. Therefore, it can be considered as a premeditated use of disruptive activities or related threats thereof in cyber space with the objective to further certain social, ideological, religious, political or any other related objectives in order to intimidate anyone to furtherance of such objective.

It may be briefly stated that, the cyber terrorism is the crime where in a person or association of persons are indulged in any form of violence or disruption of services or mode of communication required to the community or damaging property with the help of computer technology in order to terrorize and threatening the peace and comfort of the society by putting them in the constant fear. Such criminal activities are committed mainly by coercing or over awing the government formed by law or by endangering the sovereignty or the integrity of a nation.[227]

The threat from the groups of cyber terrorists has becoming the alarming dimensions mainly with such international terrorist groups working from the countless source in order to attain their negatively conceived extremist goals, *Al-Qaeda* is one among the prominent international terrorists group which has drawn attention in the recent times. It is mainly opposing to all the 'non-Islamic' communities and regimes and which is strongly anti-western. Its main target is to re-establish the Muslim States throughout the

[227] Cyber threats to national security | Public Website, , https://www.cpni.gov.uk/cyber (last visited Jul 25, 2020).

Persian Gulf. It has established a concrete communication network based on the internet network which is to be used by them as a weapon.[228]

Besides, the terrorist group like Al-Qaeda, there are a few other notorious international cyber terrorist associations operating in various parts of the world, to be mentioned as, *Armed Islamic Group*[229], which operates mainly in the areas of Algeria and France, other is *Aum Shinrikyo*[230] operating in Japan and Russia and Hamas which marks its presence also in Israel and Jordan.

The master minds of such cyber terrorism resort to launch really massive attack based on the network, which may be mainly in the face of the defacement of website or the denial of service attacks or secret widespread distribution of firmware or viruses throughout their computer network and therefore, just sabotage their entire system.

Cyber terrorism has potentially disastrous effects resulting to 'Mass destruction', thus, the private sector's co-operation is also an utmost necessary effort in assisting the law enforcement agencies for the purpose of analyses, detection, identification and prevention of such problem of cyber terrorism and restoration of law and order in the society.

2. Online Trafficking:

Online trafficking may be tending to happen in different forms. It may be trafficking of drugs, human beings' arms and ammunitions, weapons, wild animals etc. These forms of trafficking are now a day going on unabated because they are carried on under the cover of pseudonyms. Recently, a racket was busted in Chennai where the prohibited dangerous drugs were being sold under the pseudonym i.e., *honey*.[231]

[228] New Cyber Warning: ISIS Or Al-Qaeda Could Attack Using 'Dirty Bomb,' , https://www.forbes.com/sites/zakdoffman/2019/09/13/cyber-dirty-bomb-terrorist-threat-is-real-warns-us-cyber-general/#1a9d78c5679f (last visited Jul 25, 2020).

[229] ARMED ISLAMIC GROUP | United Nations Security Council, , https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list/summaries/entity/armed-islamic-group (last visited Jul 25, 2020).

[230] Sally Chapman, *Aum Shinrikyo: What Did We Learn?*, HOMELAND SECURITY DIGITAL LIBRARY (2012), https://www.hsdl.org/c/aum-shinrikyo-what-did-we-learn/ (last visited Jul 25, 2020).

[231] *On 'cyber trafficking' and the protection of its victims*, VÖLKERRECHTSBLOG (2017), https://voelkerrechtsblog.org/on-cyber-trafficking-and-the-protection-of-its-victims/ (last visited Jul 25, 2020).

3. Money laundering and other Financial Crimes:

Online financial crimes include cheating, credit card frauds, window-to-window money laundering etc. In present times, internet fraud and online cheatings are the most lucrative unethical businesses that are being carried on unabatedly through the help of the cyberspace. They may be assumed in different forms. Some of the recent practices comes as famous cases of online cheatings that have bought to the light are those pertaining to contractual deceit, fake, offering of jobs, mark sheet scandals etc.

The cyber money laundering is a common species of financial crime. It means a fraudulent way of misappropriating the credit card numbers of several persons when their monetary transactions are happening and then the transferring the money in one's own account or to using it for one's own benefit.

The term ‘money laundering’ was used for the first time in a legal context in the ‘Watergate Scandal’ case of United States in the year 1973 and it is meant, “a process of converting money arrived from illegal activities into a legally consumable form. Thus, money laundering is a cybercrime in which the money is illegally appropriated while it is in transit.[232]

4. Sale of the unlawful articles:

These form of offences include selling of unlawful articles through the use of internet, such as, sale of narcotics, weapons, wild-life-skins antiques etc. through updating information on their websites, auction websites or simply by using e-mail communication are all covered under this category of computer crime. For instance, there were many of the auction sites in India are believed to be selling the cocaine in the name of honey and thus, carrying on sale of prohibited articles illegally. The illegal wild animals selling on the internet is a recent phenomenon, which also the cyber criminals consider to be one of the most lucrative business. Though, the present international law considered to have a well-equipped mechanism for the purpose of settlement of cross border disputes relating to any international commercial transactions but there being absence of effective legal framework

[232] James Chen, *Money Laundering*, INVESTOPEDIA , https://www.investopedia.com/terms/m/moneylaundering.asp (last visited Jul 25, 2020).

for regulating wildlife trade on internet at the international level, the sale of wildlife items through the internet is a serious point of concern for the law enforcement agencies of various nations including India.[233]

5. Online Gambling:

The professional and habitual gamblers have number of opportunities to satisfy their craze for gambling on the internet. Presently, there are millions of websites hosted on the servers abroad that provide the online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering. Presently, almost about the 1500 internet gambling sites being available, all that one has to do is to wager on a multitude of casino games or sporting events by online cash payment at credit card facility and set up an account. The rapidly growing number of online gambling sites clearly indicates that gambling has becoming a potential source of addiction for the technology friendly persons, especially, the youths though they may at times be looted, deceived or cheated by some fake gambling sites.[234]

6. Forgery:

System network provides sufficient scope for the criminals to forge the documents with the help of sophisticated computers, printers, scanners etc. counterfeiting the currency notes, postal, revenue stamps and even mark sheets etc., can easily be done through these network devices.[235] In fact, it has considered as a lucrative business for professional criminals to target the needy customers, especially, unemployed persons, students etc. and extract the money by providing them with duplicate documents or fake appointment letters, mark sheets etc. The aforesaid statements about the classification of cybercrimes sufficiently highlights the enormity of these offence and their damaging effect on the individual person's government commercial or the business organizations, banks

[233] Sale of Illegal Articles, , DIGITAL FORENSICS (4N6) (2016), https://www.digital4n6journal.com/sale-of-illegal-articles/ (last visited Jul 25, 2020).

[234] Cyber Crime - Online Gambling - Internet, Encryption, Criminal, and Communication - JRank Articles, , https://law.jrank.org/pages/11989/Cyber-Crime-Online-gambling.html (last visited Jul 25, 2020).

[235] Cybercrime - Counterfeiting and forgery, , ENCYCLOPEDIA BRITANNICA , https://www.britannica.com/topic/cybercrime (last visited Jul 25, 2020).

and financial organizations industrial enterprises and the society as a whole. The problems will continue to escalate with the new enhancements in the technology.[236]

The requirement of the time, therefore, is to implement a uniform international cyber law for the prevention and restriction of cybercrime which would be universally acceptable by all the countries around the world. By the 'European Convention on Cybercrime'[237], it also has emphasized the importance for pursuing any common criminal policy aimed at the protection of society against the Cybercrimes and the criminals as also for co-operation between all the countries in order to combat this worldwide menace.[238]

[236] *Ibid.*

[237] The Council of Europe's Convention on Cybercrime, , https://epic.org/privacy/intl/ccc.html (last visited Jul 25, 2020).

[238] Cybercrime - Counterfeiting and forgery, *supra* note 221.

CHAPTER 6

JURISDICTION FOR CYBER CRIMES: PUNISHMENTS AND PREVENTIONS

The first question which is to be addressed is that what is cyberspace? It is possible to quest towards a functional answer towards this question. Practically, cyberspace is to be considered as a place. It is a place where chats and the Web pages are posted for every person in the world to see, if they are able to find them. The Supreme Court of United States has opinion on the Internet that, it contains language that makes the one hopeful that U.S. Courts will accept the legal metaphor of cyberspace as an area outside national boundaries: "Taken together, these tools constitute a unique mode- known to its users as 'Cyberspace'[239]- located in no certain location but available to anyone, anywhere in the World, with the access to the internet. In the territory of the International Law a type of territory which can be called as the international space." Currently, there are three of such international areas: Antarctica, the outer space, the high seas for the jurisdictional analysis, cyberspace.

6.1. PRIVATE DEFENCE IN CYBER SPACE:

The upcoming advent of internet technology is double edged sword, which may be used for the destructive as well as constructive work. Therefore, the future of many ventures are based upon the benign or vice intentions, of the person dealing with it, as the case may be, or with the technology. For instance, a wrongful intention promoted in the form of hacking, data-theft, virus attacks, etc., may bring only the disastrous outcomes. However, these approaches may also be used for verifying the authenticity, reliability, safety and the security of one's network based or technological device, which has been firstly, relied upon and affirmed for providing the security to any particular organisation. For example, the builder of the "Sasser-worm" has been recruited as a "security software programmer" by a famous German firm, so that he can build the stronger firewalls, which may prevent the suspicious or suspected files from entering into the computer systems. This exercise of recruiting those professionals, who are responsible for causing such havoc

[239] Cyberspace | communications | Britannica, , https://www.britannica.com/topic/cyberspace (last visited Jul 25, 2020).

and to be noted for nuisance which is the recognition of the growing and inevitable need of “self-protection”, which may be recognized in all the countries across the world, moreover, a society without any protective defence in the form of “self-help” may not be visualized in the present technological era. The content or service providers, across the world, have mostly favored the proposed regulations and legislations in their respective nations, which may allow them to restrict the copyright infringer’s computers. In certain countries, the software designers and developers have unconditionally supported the legislations, which made them able to remotely disable the computer violating the terms and conditions of the license facilitating the use of such software. This area may, however, given birth to a discussion about the desirability, availability and the legality of a law providing for a disabling effect to such “malware”. The issue is further made complicated due to lack of any uniform law solving the “jurisdictional problem”. The Internet recognizes no boundaries, therefore, the cyber attacker or offender may belong to any part across the whole world, thus, the law of the offended country may not be that efficient. This has enhanced the requirement for a “techno legal” solution rather than any pure legal recourse in the present technological era.[240]

6.1.1. The need of Private Defence:

The deadliest and the most destructive consequence of this helplessness is the emergence of the problem of “cyber-terrorism”. The adversarial definitions and methods of terrorism have recently taken a new dimension, which could be considered as more destructive and deadly in the nature. In the age of information technology, the new terrorists have equipped themselves with an expertise to produce the deadliest combination of weapons with the latest technology, which if not appropriately protected in the due course of time, will take its own toll. The losses so resulted would be almost irreversible and to be catastrophic in nature. To be precise, world is now facing the worst form of terrorism popularly known as “Cyber Terrorism”[241]. The term “cyber-terrorism” extensively includes an intentional adverse and the dangerous application of the

[240] Private defence in cyberspace, , http://www.crime-research.org/articles/private-defence-in-cyberspace/ (last visited Jul 26, 2020).

[241] Oliver Wyman, *Global Cyber Terrorism Incidents on the Rise*, https://www.mmc.com/insights/publications/2018/nov/global-cyber-terrorism-incidents-on-the-rise.html (last visited Jul 26, 2020).

information technology for producing and creating the destructive and negative effects on the property, of others, whether it is tangible or intangible. For example, the act of hacking to any computer system and then extracting or deleting the most useful and the classified working information of the rival competitor is a part and parcel of cyber terrorism. The definition of cyber terrorism cannot be made particularly exhaustive as the nature of crime is such that it must be remained to be inclusive in nature. The impact of cyberspace recently, is such that new methods and technologies are invented regularly; thus, it may not advisable to put the definition in a strait jacket formula like uniform or pigeons hole. In fact, the foremost effort of the Courts needs to be to interpret the definition as liberally or practically as possible so that the menace of such cyber terrorism can be handled stringently and with a punitive touch. The regulations dealing with cyber terrorism is, however, not sufficient to meet the pre-carious objectives of these cyber-terrorists and really needs a fresh rejuvenation in the light and context of the recent developments all across the world. The laws have to take care of the main issues originating at the international level because the technology, through which such terrorist activities are carried out, considers no boundaries. Therefore, a cyber-terrorist can destroy the economic and technical structure of a country from a place with which a country does not have any connectivity or reciprocal arrangements, including any extradition treaty. The only protection in such a situation that can be sought is to use the latest technology in order to counter such problems, Therefore, an appropriate combination of the latest security technology and regulation dealing with such acts of cyber terrorism is the need of the hour.[242]

6.1.2. The Concept of Private Defence:

In India, there is no particular law, which is specifically dealing with prevention of malware through the private defense. Therefore, the existing analogous regulations need to be applied in the purposive manner. The below mentioned provisions of the Indian Penal

[242] Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence - Media, Telecoms, IT, Entertainment - India, , https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence (last visited Jul 26, 2020).

Code[243], which is a substantive law dealing with the offences in India, are of high significance while dealing with and tackling the use of such malware thorough the use of private defence.

(i) Section 96 of the Code[244], states and declares that, nothing is an offence, if it is done in the exercise of the right of private defence. This section recognizes that the principle of self-help which is to be considered as the just, fair and reasonable in all the countries across the world.

(ii) Section 97 of the Code[245] enumerates that, every person has a right, subject to the restrictions contained under Section 99[246], to defend, firstly: his own self i.e., his own body and the body of any other person against any offence affecting the human body. Secondly, the property, whether it is moveable or immoveable, of himself or of any other person, against any of act which is considered as an offence falling under the definition of theft, robbery, mischief or criminal trespass. This part of the section mainly deals with the right of a "third party" i.e., to protect the property of another, besides, protecting his own property. Thus, a public-spirited person has a right to self-help by helping the victims of such malware. For example, netizen, who possess expertise in protecting computers from the viruses may make a programme, which has a potential to control the virus moved on the internet and may launch the same on it. In such a situation, the person executing such malware cannot complain that such third party has no ground to feel aggrieved and has no any right to retaliate. Such form of action on the part of that public-spirited individual is morally, equitably and legally justified and will be protected by this section. This is a benign concept and it requires the most liberal, purposive and updating interpretation.

(iii) Section 99[247], among other things, provides that there is no right of private defence in cases in which there is time to have recourse to the protection of the

[243] Indian Penal Code, 1860 | Bare Acts | Law Library | AdvocateKhoj, , https://www.advocatekhoj.com/library/bareacts/indianpenalcode/index.php?Title=Indian%20Penal%20Code,%201860 (last visited Jul 26, 2020).
[244] *Ibid.*
[245] *Ibid.*
[246] *Ibid.*
[247] *Ibid.*

public authorities. Further, it provides that the right to private defence in no case extends to the inflicting of more harm than it is necessary to inflict for the purpose of defence, i.e. the principle of proportionality. It is suggested that this section applies to offences involving human beings as such and not the results created due to acts or omissions of the human beings. Thus, the requirement of taking recourse to public authorities arises only when the following two requirements are fulfilled:

a) There must not be any apprehension of death or grievous hurt (in that matter the concerned person is left with no choice but to the instant life-saving action) by the omission or act in question, and;
b) Such omission or act must originate from an active physical involvement or participation of human agencies and it should include and not be limited to any act or omission unsupported by its physical presence.[248]

The reference of Section 103[249] along with Section 99 further strengthens the argument. The section 103 enumerates that ‘the right of private defence of property’ furthers, under the limitations mentioned under Section 99, to the voluntary causing of death or of any other form of wrong or harm to the wrongdoer, if the offence of robbery, house breaking at night, mischief through fire at certain properties, theft, or house breaking or trespass, arc attempted to be considered as committed under such circumstances as may be reasonably cause apprehension that death or the grievous hurt will be the outcome, if such given right of private defence is not fully exercised. The focused readings of these sections reveals that they are mainly observing the operation of private defence vis-a-vis human being's active and main physical involvement and not in the sense of malware. This position is made crystal clear if it is to be read with the definition of ‘death’ under section 46 of the Code[250], which briefly explains that the word ‘death’ denotes death of a human being, unless the contrary is shown from the context. It would become the absurd results,

[248] Cyber Crimes Under The IPC And IT Act - An Uneasy Co-Existence - Media, Telecoms, IT, Entertainment - India, , https://www.mondaq.com/india/it-and-internet/891738/cyber-crimes-under-the-ipc-and-it-act--an-uneasy-co-existence (last visited Jul 26, 2020).

[249] Indian Penal Code, 1860 | Bare Acts | Law Library | AdvocateKhoj, , https://www.advocatekhoj.com/library/bareacts/indianpenalcode/index.php?Title=Indian%20Penal%20Code,%201860 (last visited Jul 26, 2020).

[250] *Ibid.*

if it is argued that the briefing of the sections in the present situation is talking about the 'death of the computer' or of the 'operating system'.[251] Moreover, it may be considered as unreasonable, in fact, unrealistic and imaginary, to point out that for protecting one's computer from malware, almost every time, recourse towards public authorities has to be taken. In fact, the main contention for providing the regulations concerning the private defense is that, the state may not protect the life and property of all the citizen at all times. Therefore, as a measure of public policy and of practical convenience, the concept of self-help has been given a moral, equitable and also a legal sanction. Even though, under the code there is an inherent and patent differentiation between section 99 and section 103. Section 103 is subject to the certain provisions of section 99. It is mentioning about the taking recourse of public authorities, when the act or omission 'does not' reasonably leads to the apprehension of death or of grievous hurt. It implies that, if there is an immediate apprehension of death or of the grievous hurt, then the remedies to the public authorities need not to be taken. This may be considered as practical, as it satisfies the tests of the common sense, because any person cannot approach to the public authorities after his or her death, which may be resulted due to the immediate peril of life. Additionally, no other useful purpose may be served by contacting the public authorities, if such grievous hurt has already been afflicted on them. In fact, if there is a threat of the death or grievous hurt, the right of private defence can be exercised even against a public servant, who may though be acting in a good faith under the color of his office is not to be strictly justifiable by the law. It should be applauded that, no malware can cause any form of direct physical injury or apprehension towards any physical injury, which necessitate the recourse to public authorities within the meaning of section 99 of the Code[252]. Therefore, it may assuredly be concluded that recourse to self-help can be taken up under section 103 of the Code without consulting the concerned authorities, since it does not involve the potential and active physical presence of the human body. This is also in consonance with the basic theme and object of the idea of self-help and the practical and current requirements of law and its

[251] Computer Vandalism, , WWW.KASPERSKY.CO.IN (2017), https://www.kaspersky.co.in/resource-center/threats/computer-vandalism (last visited Jul 25, 2020).

[252] Indian Penal Code, 1860 | Bare Acts | Law Library | AdvocateKhoj, , https://www.advocatekhoj.com/library/bareacts/indianpenalcode/index.php?Title=Indian%20Penal%20Code,%201860 (last visited Jul 26, 2020).

regulation of the society. However, the enforcement of Section 99 is not, completely excluded while exercising the rights relating to private defense under Section 103 of the Code. It must also be highlighted that section 99 also recognizes the 'principle of proportionality' among the other things as well. This specifically implies that the proposed damage given by the technological property holder must commensurate directly with the nature and the gravity of the threat. Therefore, the damage, if at all caused, it is considered to be so, such damage is to be reasonable, proportionate and not to be unduly harsh. At the moment it exceeds the limits, which may be deemed to be seem appropriate by a reasonable person, it may directly offend the benign objects behind the section 99 of Code, and may finally become illegal. Therefore, to this extent, and in the same consensus to this sense only, Section 103 is in a way subject to the section 90 of the Code, this interpretation also fulfils the direct conflicting requirements of private defence of information technology and the equal proportionate action required to be enforced by the person executing such private defence. This is certainly not an end of this matter. Sections 99 and 103 needs to be interpreted also in the light of Section 105 of the Code[253] to make them more meaningful. Section 105 of the Code also enumerates that, the right relating to the private defence of property commences as soon as a reasonable speculation of the danger to the property commences. There are certain chances that, a particular malware may not give rise to such apprehension at all because of its networking, programming and operational specifications. In that matter, the owners of the information technology come to into the knowledge when the targeted loss has already been done. In that situation, no potential purpose will be served by contacting any public authorities, as they already cannot undo what has already been happened. In order to reduce such an eventuality, it is really important and required to adopt certain precautionary technological measures, since, the beforehand prevention is always better than the problematic and expensive cure. As a concluding remarks, it may be keenly highlighted that, by the virtue of Section 40 of the Code, the right relating to private defence is to be allowed against offences committed under certain special laws as well. In India, Information Technology Act, 2000 (ITA) is considered as a special law made enforceable to matters mainly pertaining to the information technology. Therefore, the provisions relating to private defence may also imprints their color from it. In case there is a clash

[253] Indian Penal Code, 1860 | Bare Acts | Law Library | AdvocateKhoj, , *supra* note *242.*

between the provisions of the code and the IT Act, obviously, the latter will prevail. Fortunately, as of now, on practical grounds, there is no conflict between the provisions of the Code and IT Act, hence, the interpretation given to the sections, as already mentioned above, along with a purposive interpretation of such provisions relating to the IT Act would be enough in order to take care of the principles for governing the principles of private defence relating to the technological property, which also includes the Intellectual property rights stored in it.[254]

6.2. PREVENTION AND PUNISHMENTS RELATING TO CYBER SPACE:

The evolving dangers through the crimes committed against networks of computers or against any specific information preserved in computers is becoming to claim some spotlight in certain national capitals; In most of the countries across the world, however, prevalent laws are more likely to be not enforceable towards such crimes. This lack of legal enforceability means that any organizations and governments must depends mainly on the technical measures in order to defend themselves from those who would steal deny access to or destroy the valuable information.

6.2.1. Offences Punishable Under the Information Technology Act, 2000:

The rising cases of cybercrimes due to growing development of network based and computer based technology necessitated creation and enforcement of different law for prevention and control of these offences. Thus, the enactment body of India i.e., finally enacted the Information Technology Act, 2000[255], as a regulatory measure to deal with the cyber offences in an effective manner. This Act is mainly based on the idea taken from UNCITRAL Model Law on e-commerce, of the year 1996[256], in furtherance to the resolution of United Nations General Assembly proposing and requesting the member states to consider it analyze, enact or to take revision of their laws in order to make certain

[254] Information Technology Act 2000 | Ministry of Electronics and Information Technology, Government of India, , https://www.meity.gov.in/content/information-technology-act-2000 (last visited Jul 26, 2020).
[255] *Ibid.*
[256] Rishabh Aggarwal, *UNCITRAL Model Law on E – Commerce*, LEGAL BITES - LAW AND BEYOND , https://www.legalbites.in/uncitral-model-law-on-e-commerce/ (last visited Jul 26, 2020).

uniform atmosphere for the purpose of regulating any e-commerce across the world. Thus, the main contention of this Act is that, “to provide legal validation for the purpose of transactions carried out through the electronic medium, data, internet and any other means of electronic based communications mainly referred as to the e-commerce as an alternative to physical based methods of communication and storage of the information in order to support and enhance the electronic filing of documents”. In the view of this target, the Act also incorporates certain provisions for the prevention and appropriate control of offences which are the result of e-governance and e-commerce. The near relevant provisions are contained in Chapter IX and XI of the said Act.[257]

i) Punishment of Cyber Crimes:

Penalty for damage of computer, computer system etc.:

If without the due permission of the owner or creator or any person who is in charge of a computer, computer system or computer network, any person-

a) Entry or secures access to such network or computer, computer system or any stored data;

b) Saves, extracts or copies any potential data, computer related database or any potential information through such computer, storage system or the network based system including the information or data kept or safely stored in the removable storage medium of system;

c) Mainly causes to be introduced the potential system contaminant or software virus into any computer, computer system or computer network;

d) Damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other program residing in such computer, computer system or computer network;

e) Destroys or any action leads to destruction of any system, computer body or computer network;

f) Restricts or causes the restriction to access of any person authorized to access any computer, computer system or computer network by any means;

[257] Information Technology Act 2000 | Ministry of Electronics and Information Technology, Government of India, *supra* note *242.*

g) Provides any help to any person in order to facilitate the access of a storage, computer system or computer network in contravention from the guidelines of the provided Act, rules or regulations made thereunder;

h) Monetize the service availed of by anyone to the account of another person by hampering the or breaking any computer, computer system or computer network.

i) He shall be made liable to pay damages through the appropriate compensation not exceeding the amount one crore rupees to the person so affected.[258]

Section 43 (a) of The Information Technology Act, 2000[259] has provided the authorized access to any computer, storage system or any network without the due authorization of the owner or the person who is in charge, punishable without any direct reference to the malafide intention and nonetheless, there is no any loss, which may or may not have been occurred to the owner or person in charge of such system. Therefore, it is well enough to conclude by proving that the hacker or intruder has accessed or secured access to the system, victim's computer or his network, without any due permission of the victim or the person in charge of such system. Any financial or other such kind of loss is not required to be inferred by the victim in order to claim damages under this section, but the quantum and the magnitude of the damage caused to the victim of such attack may act as a relevant incident to determine the appropriate amount of damages which may be enforced under this said section.

Clause (b) of section 43, provides the provision which states that downloading, extracting or copying any potential data, database saved in system storage or any other relevant information from such system or through the unauthorized access to the computer network a contravention. It ultimately aims to protect the copyright of the individual over his creation through and on the digital medium. This process of downloading, extracting or copying of any potential data etc. can be held or preserved in any removable storage

[258] Penalty for damage to computer, computer system, etc. | Information Technology Act | Bare Acts | Law Library | AdvocateKhoj, https://www.advocatekhoj.com/library/bareacts/informationtechnology/43.php?Title=Information%20Technology%20Act&STitle=Penalty%20for%20damage%20to%20computer,%20computer%20system,%20etc. (last visited Jul 26, 2020).

[259] Section 43A of Information Technology Act: Compensation for failure to protect data, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-43a-compensation-for-failure-to-protect-data/ (last visited Jul 26, 2020).

space including Compact Disks, DVDs or the floppy disk etc. Even, if anyone secures the access to any computer with the permission of the owner or the person in charge but downloads, copies or extracts any data, it protects the integral right of the owner.[260]

Clause (c) of the section 43 provides the brief outline or causing to introduce any form of data contaminant or any dangerous virus such as worms, logic bombs, Trojan Horse virus programs etc. into any storage space or computer system or any computer network is a contravention for which charge of fine up to the tune of one crore rupees may be claimed by the victim, owner or person in charge of such storage space, computer system or such computer network. The most famous instance is the virus of 'love bug' formed and disseminated in the year 2000 which badly affected and damaged various storage systems and computers. There is a famous saying that: "Do not send a man where you can send a bullet". This saying cap be modified in the cyber world as "Do not send a bullet where you can send a virus". It is fairly not relevant to take into account that the accused person was actually not aiming to attack the computer, computer system or computer network of the victim but of somebody else and it was by mere chance that the system of the victim was affected. Nor it is essential to infer and prove that the person had any sort of malafide intention while outlining or causing to introduce the computer containment or the virus. This clause (c) of the said section needs to be read conjointly with the provided explanations such as (i), (iii) and (iv) of this section. This sub section also tends to covers about the person, whose system get infected by a virus or contaminant without person's knowledge and that person provides or sends the infected file to some other person without any of malafide intention or knowledge Thus, it becomes important to get and install any safe antivirus software for the protection of system against any form of dangerous worms or virus.[261]

Further, clause (d) provides the causing loss or attempt to cause breaking or damage to any computer, Computer system or computer network, data, computer database or any other program residing in such computer, computer network or computer system as a

[260] Section 43 of Information Technology Act: Penalty and Compensation for damage to computer, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-43-penalty-and-compensation-for-damage-to-computer-computer-system-etc/ (last visited Jul 26, 2020).

[261] *Ibid.*

cyber-contravention. The breaking or loss includes the damage to the software as well as to the hardware. Such loss may be done physically or virtually through the spread of virus etc. or through any other medium.[262]

Clause (e) of the said section provides the disruption and attempt to cause disruption to storage space, system or the network as a cyber-contravention. The provisions mentioned in the clauses (c) and (d) may in the certain instances be reason of the said disruption of storage space, system or any potential computer related network.[263]

Clause (f) provides the absolute denial or attempt to deny access for the system storage, computer related system or the computer network to any authorized person through any means. Such restriction for access may be either physical or virtual. The virtual restriction on access may be, either by changing the user password, User's ID address etc. or through some other means. It includes “Denial of Service Attacks”, where the cyber attacker blocks the authorized users from visiting the targeted sites.[264]

Clause (g) enumerates that providing assistance to any person for even making to access to any storage space, computer system or computer network in contravention to the law is a cyber-contravention. Thus, any person who helps another person to access any computer, computer system or computer network in violation to the provisions of this Act or rules or regulations made thereunder is guilty of committing cyber contravention.[265]

Clause (h) states that any person who charges the service availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network commits contravention. This clause mainly provides protection against theft of internet hours or any other misappropriation of fraud where by the cybercriminal by changing, tampering or manipulating the password, user's ID details etc. attains the benefits of the services taken by the needful person.[266]

[262] *Ibid.*
[263] *Ibid.*
[264] *Ibid.*
[265] *Ibid.*
[266] *Ibid.*

The Information Technology (Amendment) Act, 2008 finally provided a new section 43A[267] towards the Parent Act, by providing the provisions of compensation in case of failure to protect data. Whereby, the organization (i.e. corporate or firm) dealing, possessing or controlling any sensitive potential data or information in a storage resources which it possesses, owns or operates, is negligent in applying and implementing the potential protective practices and guidelines and thereby causes drastic loss or unethical gain to any person, such organization shall be ultimately made liable to pay damages or requisite compensation to the victim so affected.

Penalty if Failure to furnish Proper Information Return:

If anyone, who is made under this Act or any related rules or regulations required thereunder to-

a. provide any document, report or return to the controller of such certifying legal authority does not furnish the same, he or she shall be liable for a penalty not exceeding the amount of one lakh and fifty thousand rupees towards each such failure;
b. file or provide any return or furnish any related information, books or any other related documents under the specified time, therefore, as per the provided regulations, does not file the return or to furnish the said documents within such specified time, therefore, as per the provided regulations, he or she shall be liable for a penalty not exceeding the amount of five thousand rupees for each day from which such failures tends to continue;
c. record or maintain books of accounts or even fails to maintain them, he or she shall be made liable for the penalty not exceeding the amount of ten thousand rupees for each such day from which such failure tends to continue;

This section also directs the person who is required to furnish any document, return or report, in order to file the return or to provide any such relevant information, books or other documents towards the said concerned authority or to keep the books of accounts or

[267] Section 43A of Information Technology Act: Compensation for failure to protect data, *Supra* note 258.

although records, but fails to do so, to be made liable for such contraventions and made liable by providing the monetary punishments towards it.[268]

Residuary Penalties:

This section provides the provisions to direct the person who is required to duly provide any such document, return or report, in order to file the return or to provide any such relevant information, books or any other documents to the said concerned authority or to keep the books of accounts or although records, but fails to do so, to be made liable for such contraventions and to be made liable by providing monetary punishments for the same.

If any person contravenes any such provided rules or regulations made and enumerated under this said Act, but for such contraventions, no separate penalty has been provided under the Act, such rules or regulations provided thereunder, thus, such contravener shall be made liable in a way to pay appropriate compensation which may extend to the amount of rupees twenty-five thousand but not more than the mentioned amount.[269]

Tampering with Computer related Physical Documents or E-Documents:

Whoever, by knowingly or due to any wrongful reasons conceals, alters or destroys or by wrongful intentions or by knowingly causes some another to conceal, alter or destroy any potential computer source code used for the purpose to compute, for computer programs, related system or computer network, when such source code of the computer is required to be kept confidential from public or to be maintained by law for the time being in force, shall be made punishable by way of imprisonment for the period up to three years

[268] Section 44: Penalty for failure to furnish information, return, etc, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-44-penalty-for-failure-to-furnish-information-return-etc/ (last visited Jul 26, 2020).

[269] Residuary penalty | Information Technology Act | Bare Acts | Law Library | AdvocateKhoj, , https://www.advocatekhoj.com/library/bareacts/informationtechnology/45.php?Title=Information%20Technology%20Act&STitle=Residuary%20penalty (last visited Jul 26, 2020).

or with the fine which may extend up to the amount of rupee two lakh rupees, or with the both.[270]

Hacking to the system's storage or network:

A person is said to be charged for committing the offence of hacking, when:

a. He acts which results to cause wrongful loss or damage to the general public or to any person.
b. By destroying or deleting or altering any potential information residing in the computer resource or by significantly reducing its working value or utility or affecting it injuriously through any harmful means.
c. From the deceitful intention or knowledge that he may likely to cause such wrongful loss or adverse damage to the general public or to any particular person.[271]

Any such person who tends to commit such mentioned offence of hacking is called hacker. In the general parlance, the term 'hacking' is also used as a synonym for the 'unauthorized access to computer' or for the 'computer system trespass'. In order to constitute the offence of hacking, however, in terms of section 66, certain additional requirements under such section should also needs to get fulfilled.

This offence of hacking may have remained to be committed with respect to both, the tangible and intangible assets. The tangible assets mainly include the hardware bodies or components relating to the computer resource(s) such as, system layout boards, whereas, the intangible assets mainly include the informations shaped through the process and in the form of some electronic, magnetic or optical impulses.

Although, this section 66 does not include the hackers, who does not have any sort of criminal intent or knowledge in order to cause any wrongful loss or any damage. The act f hacking per se, which does not have any guilty mind and the malice does not to be made punishable under section 66 of the Act. It would, nevertheless, to be made punishable under

[270] Cyber Crime Lawyer in Delhi.India, *section 65 of IT Act 2000. Tampering with computer source documents.*, CYBER CRIME LAWYERS IN DELHI,INDIA (2013), https://cybercrimelawyer.wordpress.com/2013/05/16/section-65-of-it-act-2000-tampering-with-computer-source-documents/ (last visited Jul 26, 2020).

[271] Section 66 of Information Technology Act: Computer Related Offences, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-66-computer-related-offences/ (last visited Jul 26, 2020).

section 43 (a) without any due regards towards the intention of such hacker of any system or network.

Also, sub-section (2) prescribes about the punishments towards the hacker, even though there may no benefit would have been accrued by the hacker out of such illegal acts committed by him.[272]

Publishing the obscene information in electronic form:

Any person who publishes or transmits or likely to be published any document of electronic form, any potential matter which is lascivious or appeals to the interest or if its effects is such as which makes it to deprave or corrupt the reputation of persons who are likely, having regard to all the relevant conditions, to see, read or to hear the matter stored or may be embodied in it, shall be punished with the first conviction of the imprisonment either as per description of a term which may be extend to the period of five years along with the fine which may extend to the amount of one lakh rupees and to the event of second or in the case of subsequent conviction with the charges of imprisonment for either description for a term which may be extend to the period of ten years and along with fine which may also be extend to the amount of two lakh rupees.

The important ingredients of Section 67, are:

1. Creation, Transmission or Publication of any material in the electronic form.
2. The said material needs to be lascivious or should appeal to the prurient interest of the potential audience or the target of such material to be such that it should tend to deprive or to corrupt the minds of such potential audience.[273]

Under this section, the act of publication and transmission of the obscene information is prohibited and the such transmitter would be liable and to be prosecuted and punished accordingly. The act of publication or such transmission in an electronic form which includes the dissemination, distribution, circulation and storage of such potential

[272] Section 66 of Information Technology Act: Computer Related Offences, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-66-computer-related-offences/ (last visited Jul 26, 2020).

[273] Section 67 of Information Technology Act: Punishment for publishing or transmitting obscene material in electronic form, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-67-punishment-for-publishing-or-transmitting-obscene-material-in-electronic-form/ (last visited Jul 25, 2020).

information or data in an electronic form. Therefore, the downloading of material is also covered within the area of this section.

The act of publication or such transmission of the obscene material in an electronic form is to be considered as offence but the act of merely browsing or surfing the obscene material over the internet or possessing such material in the privacy of one's home is not an offence. It is only, when the material is disseminated, published or transmitted in an electronic form; it becomes an offence under section 67 of the Act.

Such act of transmission alone is enough to label these act as an offence, if the basic ingredients mentioned in section 67 are found to present. The plea that connect the audience of the transmission was desired to be the picked-up people is unsustainable, if others are likely to have access to such material.

The material which constitutes the obscenity, or in the words of section 67, that the material which can be considered to be lascivious or which appeals to the sexual interest or having such effects which tend to deprive or to corrupt the persons who are likely, have regard to all relevant chances, to observe, see or to collect the material stored or embodied in it, to be considered as a question of fact.

In the famous case of *Ranjit Udeshi v. State of Maharashtra*[274], where the Lady Chatterley's Lover written by D. H. Lawrence which was held ‘obscene’ as it had, according to the statement of Supreme Court, a negative tendency to “deprive or to corrupt by the immoral influences”, the persons into whose hands the book was "likely to fall". The Supreme Court stated that, “The word obscenity is really not vague because it is a word which is well understood even if persons differ in their attitudes to what is obscenity and what is not”. The Court has held that the following matters to be considered obscene.

1. which depraves and corrupts those whose minds are open to such immoral influences.
2. which suggests thoughts of a most impure and libidinous character.
3. which is hardcore pornography.

[274] *Ranjit Udeshi v. State of Maharashtra – I: Obscenity, morality and public interest*, INDIAN CONSTITUTIONAL LAW AND PHILOSOPHY (2013), https://indconlawphil.wordpress.com/2013/08/04/ranjit-udeshi-v-state-of-maharashtra-obscenity-morality-and-public-interest/ (last visited Jul 26, 2020).

4. which has a substantial tendency to corrupt by arousing lustful desires.
5. which tends to arouse sexually impure thoughts.
6. which passes the permissive limits judged from our community standards.

As according to the Supreme Court, in the *Ranjit Udeshi case*, that such video or material was considered to be obscene which "is likely to deprive and to corrupt those people, whose minds are open to influences of this type and into whose hands the book is likely to get fall".

The Hon'ble Supreme Court also further stated that "the obscene material to be considered by itself and apparently to find out that, whether it is so gross and its obscenity so decided that it is or likely to deprave and to corrupt those, to the people whose minds are vulnerable and open towards the influences of this sort and into whose hands the book is likely to fall".[275]

In another case of *Chandrakant Kalyandas Kakodar v. State of Maharashtra*[276], the Hon'ble Supreme Court expanded the terms of the test of obscenity already laid down in Ranjit Udeshi case by stating that, "it is the foremost duty of the Court to consider the obscene matter by taking an overall view of the entire work and to determine, whether such obscene passages are or so may likely to deprave and to corrupt those people, whose vulnerable minds are open to the influence of this sort and in to whose hands the book is likely to fall and in doing so, one should not ignore the influence of such book on the social morality of our contemporary society". Therefore, it is directly implied out from such Chandrakant Kalyandas Kakodkar case that, although the obscene passage or material may appear to be, when to be considered by itself, and may not be considered as obscene by taking an overall picture of the overall work.

Whether any material is to be considered as obscene or not may be tested on the principles of local community standards and by keeping in mind the integral morality of contemporary society. The minimum benchmark so as to determine any obscene material

[275] *Ibid.*

[276] Chandrakant Kalyandas Kakodar Vs The State of Maharashtra and Ors., , LEGAL AUTHORITY , https://www.legalauthority.in/judgement/chandrakant-kalyandas-kakodar-vs-the-state-of-maharashtra-and-ors-35130 (last visited Jul 26, 2020).

is that, whether a reasonable, prudent and a person with common intellect identifies such work, partly or taken as a whole, to be obscene.

Any such act which is prohibited is which is to be done as the dissemination of any obscene material through a mode of the transmission or publishing in the electronic form. If such mode carries with it the high danger of damaging or offending the sensibilities of unwilling recipient or to exposure towards the juveniles. An appeal to the prurient interest is that which promotes to a shameful or morbid the interest towards sex. Any published or transmitted work which portrays or depicts a sexual activity in the patently offensive manner is or may creating or in a way encouraging the unhealthy obsession towards the sexual activities is called to be appealing to the prurient interest towards the sex.

Generally, the cases relating to obscenity involve the acts which are happened to be in more than one jurisdiction and such obscene contents or pornography dealers mostly to be prosecuted in a state, where such obscene content is delivered. The defendants' particular knowledge about the destination of each and every transmission is not to be necessarily emphasized to made the charges be proved.[277]

In the landmark case of *State of Tamil Nadu v. Suhas Katti*[278], the Chief Metropolitan Magistrate convicted the accused merely within seven months from the filing of the FIR for the charges under section 469, 509 of the Indian Penal Code, 1860[279] and 67 of The Information Technology Act. 2000 for publishing the obscene, defamatory and derogatory messages about a divorcee woman in the yahoo message group and forwarding obscene e-mails to others through a fake e-mail account publishing her residential telephone number for inviting the people to talk to her over phone. The publishing of such messages and such offensive e-mails resulted in disturbing phone calls to the victim in the impression that she was soliciting. The accused was finally convicted and sentenced for the rigorous imprisonment up to the term of 2 years along with fine of the amount Rs. 500/- under section 469 of IPC and one-year of simple imprisonment and with the fine of amount

[277] *Ibid.*

[278] State of Tamil Nadu Vs Suhas Katti - Cyber law case in India in Cyber laws, , FREE LEGAL ADVICE - LAWYERS FORUM , https://www.legalserviceindia.com/lawforum/cyber-laws/17/state-of-tamil-nadu-vs-suhas-katti-cyber-law-case-in-india/2238/ (last visited Jul 26, 2020).

[279] Indian Penal Code, 1860 | Bare Acts | Law Library | AdvocateKhoj, *Supra* note 242.

Rs.500/- towards the offence committed under section 509 of The Indian Penal Code, 1860 and with the rigorous imprisonment for the period of 2 years along with fine of Rs.4000/- for the offence under section 67 of the information Technology Act, 2000. All these penal sentences, although, were to run concurrently. This is considered to be the first case which resulted in conviction under section 67 of Information Technology Act, 2000 in India.[280]

Power of the Controller to provide Directions:

There are several powers provided to the Controller in order to take action to curb this menace, discussed below as:

1. The Controller may, through order, provide the direction to a Certifying Authority or to any employee working under such authority for taking such measures or to cease carrying on the activities, as specified under the orders if those are necessary to ensure that they are in accordance with the provisions of this Act, rules or any regulations made here under.
2. The people, who fails to comply ‘with the provided order under sub section (1) shall be made guilty of an offence and shall be made liable for the conviction to imprisonment for a term which not exceeding the period of three years or with a fine not exceeding the amount of two lakh rupees or with the both. The integral ingredients under this section so as to become a person criminally liable are:

a) The Controller must have, through order, directed a Certifying Authority or any employee under such authority, to take such measure or to prevent carrying out such activities as specified under the orders;

b) Such mentioned orders need to be made necessary in order to ensure that they are in accordance with the provisions of the said Act, rules or the regulations made here under; the accused must have failed to comply with such mentioned orders.[281]

[280] Section 67 of Information Technology Act: Punishment for publishing or transmitting obscene material in electronic form, , INFORMATION TECH. LAW (2014), *Supra* note 272.

[281] Power of the Controller to give directions | Information Technology Act | Bare Acts | Law Library | AdvocateKhoj, https://www.advocatekhoj.com/library/bareacts/informationtechnology/68.php?Title=Information%20Technology%20Act&STitle=Power%20of%20the%20Controller%20to%20give%20directions (last visited Jul 26, 2020).

Power for the Delegation:

The Controller can be, in writing, provide the authorization to the Deputy Controller, Assistant Controller or any other officer to exercise any of such powers of the Controller.

Directions of a Controller for Subscriber to extend facilities to Decrypt Information:

1. When the Controller is satisfied that, it is important or integral to do for the interest of the sovereignty or integrity of India, the security of the country, friendly relations with the foreign states or public order or for restricting the incitement to the commission for any cognizable offence, for reasons to be recorded in, be in writing, by order, provide direction to any agency of the Government to intercept any information transferred through any computer resource.
2. The subscriber or anyone who is in charge of any computer related resource shall, whenever communicated upon by any such agency, which has already been enumerated under sub section (1) provide all the facilities and technical facilities in order to decrypt the required information.
3. The subscriber or any related person, who does not assist the agency as referred to in the sub-section (2) shall be made punished with the imprisonment for a term which may extend to the period of seven years.[282]

The ingredients provided under sub section (1) of section 69 are as follows:

1. The Controller must have provided the direction to any agency of the Government to intercept any information transferred through any computer resource.
2. The Controller should have provided such direction on being ensured that, it is pertinent to do so towards the interest of the sovereignty or for maintaining integrity of the country, the security of the state, friendly relations with foreign states or the public order or for restricting the incitement towards the commission of any cognizable offence;

[282] Directions of Controller to a subscriber to extend facilities to decrypt information | Information Technology Act, 2000 | Indian Kanoon | Legistify, , https://www.legistify.com/indiankanoon/information-technology-act-2000/section-69-directions-of-controller-to-a-subscriber-to-extend-facilities-to-decrypt-information/ (last visited Jul 26, 2020).

3. The reasons given about such direction should be recorded in writing.

The controller has been provided with the powers to give direction to any government agency to intercept any information transferred through any computer related resource. This provided power, although, is not absolute or arbitrary but it is structured with the several protection layers so as to eliminate any scope for the abuse of power. The reasons for the direction of Controller are to be recorded in writing by him. The controller should have the reasonable grounds for the information to the satisfaction that such interception of information transferred from any computer related resources are necessary or expedient for the favorable interest of the sovereignty and towards the integrity of the country, the security of the country, friendly relations with the other foreign States, or to maintain the public order or for restricting the incitement towards the commission of any of the cognizable offence. The said section, therefore, possess the sufficient measures to maintain a check on the unfettered powers provided to the controller, if any.[283]

Although, this section provides the government agency to get intrude to the privacy of the public, it possesses the adequate measures against the unreasonable interceptions by the controller or any of such government officials, every one, without a doubt, has a right to privacy against any unauthorized interception and disclosure by anyone or any such authority, be it a controller or government officials or any such private person.

The subscriber or any of the person in charge of the computer related resources, on the directions of Controller, shall disclose the content of the communication provides all the facilities and technical assistance in order to decrypt the provided information as per sub section (2). Such assistance shall, although, be construed to provide the reasonable assistance for facilitating all the facilities and technical assistance to decrypt the information. There may be examples, where the subscriber or the concerned person may not be competent enough technically in order to provide all the availabilities and technical assistance to decrypt the information.

[283] Section 69: Powers to issue directions for interception or monitoring or decryption of any information through any computer resource, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-69-powers-to-issue-directions-for-interception-or-monitoring-or-decryption-of-any-information-through-any-computer-resource/ (last visited Jul 26, 2020).

The section 5 (2) of The Telegraph Act. 1885, is in a way resembling to this section of The Information Technology Act. 2000. It states that "On the happening of any public emergency or for the interest of public safety, the Central or State Government or may the officer, particularly authorized on this behalf by the Central or State Government, may, if satisfied that it is really integral and expedient in order to do for the interest of the sovereignty or the integrity of the country, the security of the country, friendly relations with foreign States, or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing by order. direct that any message or class of message to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transferred or received through any telegraph, shall not be transferred, or shall be interfered or detained, or shall be disclosed towards the government providing the order of an officer hereof mentioned in the order."[284]

Protected System Areas:

1. The Government may, through the notification in the Official Gazette, declare any computer, system storage or any computer network to be a secured system.
2. The Government may, through the order provided in writing, allows the persons who all are authorized to get access to the protected systems as notified under sub-section (1).
3. Any one, who secures the access of or likely to get the access to a protected system in contravention to the provisions of this said section shall be made punished with the imprisonment for either description for a term which may extend to ten years and shall also be liable with a fine in accordance with court's description.[285]

The essentials which make a person criminally liable under this section:

1. The government may have declared any computer, system storage or computer network to be a secured system.

[284] Revised SOP issued for Lawful Interception of Communication, , https://pib.gov.in/newsite/PrintRelease.aspx?relid=80829 (last visited Jul 26, 2020).

[285] Protected system | Information Technology Act, 2000 | Bare Acts | Law Library | AdvocateKhoj, , https://www.advocatekhoj.com/library/bareacts/informationtechnology/70.php?Title=Information%20Technology%20Act,%202000&STitle=Protected%20system (last visited Jul 26, 2020).

2. Such said declaration may have been prepared by the appropriate Government through the notification provided in the Official Gazette. The intruder secured access or attempted to secure access to the notified protected system in contravention of the provisions of this section.
3. The intruder should not have been permitted to get access through the notified protected system.

Any sort of attempt in order to secure any illegal access to the protected computer related system has also been made punishable under section 70 (3) of the IT Act. Therefore, it is not material to determine whether the attempt was successful or not.

Penalties for the Act of Misrepresentation under Section 71 of the IT Act:

Anyone, who makes any form of misrepresentation to, or suppresses or tries to suppress any potential fact from the Controller or the said Certifying Authority in order to obtain any license or the Digital Signature Certificate, as the case may be, shall be made punished with the imprisonment for a term, which may extend to even two years, or with the fine which may extend up to one lakh rupees, or with both. The term 'Subscriber' includes a person in whose name such Digital Signature certificate is issued.

The essentials of this section may be mentioned as:

1. The person would have made any misrepresentation to or suppressed or tries to suppress any potential fact from the controller or any of the certifying authority;
2. Such misrepresentation or suppression of such potential fact must be in relation with containing of any license or digital signature certificate.

Providing any form of incorrect and false facts may be called as misrepresentation and non-disclosure of any potential facts or information can be termed as suppression.[286]

Although, the Controller and also the authorized certifying authority contains the power to even suspend or to revoke the license and digital signature certificate of the authorized certifying authority i.e., section 25 and the subscriber i.e., section 38 respectively, but under

[286] Section 71: Penalty for misrepresentation, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-71-penalty-for-misrepresentation/ (last visited Jul 26, 2020).

aforesaid section, they may have been entrusted with such additional power in order to file the criminal charges against such applicants who may have misrepresented or the suppressed any potential facts amongst them.

As, section 68 to 71 of the IT Act, point outs the extensive power of the Controller of Certifying Authorities in regulating the functioning of the Certifying Authorities, directing subscribers to extend facilities to decrypt information, creating repository of protected system and initiating criminal charges against the certifying authorities for misrepresentation.[287]

Provisions of breach of Confidentiality and Piracy under Section 72 of the Act:

Already, as if otherwise provided in the said Act or any other form of law for the time being force, any one, who is under pursuance of any of the related powers provided under this said Act, Rules or the Regulations provided hereunder, has procured the access for any form of electronic record, register, book, correspondence, potential information, document or any other potential material in the absence of the consent of such person concerned, discloses any of such e-record, register, book, correspondence, potential information, e-document or any other potential material to some other person shall be made punished with the imprisonment for a term which may extend to two years or with the fine which to be extend to the amount of one lakh rupees or with the both.

In India, right to privacy has been took to be bracketed under the course of Article 21 of the Constitution of India. Right to privacy always shall be considered almost as a sine qua non in the Cyber world also.

Section 72 of the IT Act mainly prohibits the unauthorized disclosure of the contents of the electronic records. Privacy mainly involves two types of interest i.e., information privacy interest and another one is the autonomy privacy interest. The information privacy interest is the interest in precluding the transmission or the abuse of the sensitive and confidential information. The autonomy privacy interest is the interest in preparing the

[287] Chapter 11: Offences - Information Technology Act, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/chapter-11-offences/ (last visited Jul 26, 2020).

intimate personal decisions and conducting the personal activities without the intrusion, observation or the interference.[288]

Penalty for Publishing the False Digital Signature Certificate in Certain Particulars under Section 73 of IT Act:

1. No one shall be made publish the Digital Signature Certificate or otherwise to make it available to anyone with the knowledge that-
   a) The Certifying Authority provided under the certificate has not issued it; or
   b) The subscriber listed under the said certificate has not accepted it; or
   c) The certificate has been terminated or suspended, unless the said publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.
2. Unless the said publication is provided for the purpose of verifying or ensuring a digital signature formed prior to the termination or the revocation.[289]

6.3. PREVENTION MEASURES RELATING TO CYBER CRIMES:

Despite the presence of the penal provisions and required preventive measures provided in the Indian Penal Code and the I.T. Act, a perusal through the cybercrime statistics of the past years clearly shows that there has been no reduction in the cybercrime rate and to the contrary, such cases of cybercrimes are recording a steady rising trend. There are already several new cybercrimes showing up which really needs the high-level and improvised technical investigative and the legal techniques and skills in order to deal with them efficiently.

The crime statistics plays very important role in creating the preventive crime strategy as they possess the potential data relating to the specific crimes and the criminals which supports the criminal law enforcement agencies to make the best

[288] Section 72: Breach of confidentiality and privacy - Information Tech. Law, , https://www.itlaw.in/section-72-breach-of-confidentiality-and-privacy/ (last visited Jul 26, 2020).
[289] Section 73: Penalty for publishing electronic Signature Certificate false in certain particulars, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-73-penalty-for-publishing-electronic-signature-certificate-false-in-certain-particulars/ (last visited Jul 26, 2020).

possible use of them for the purpose of working out effective strategy to tackle such crimes efficiently.[290]

The '5P' mantra highlights the point to maintain efficient online security i.e., Precaution, Protection, Preservation, Prevention and the Perseverance.

Momentarily, in various cases, the investigation ends up with the analogy that the victim's system was attacked and there was enough evidence in order to show that substantial damage has been caused to victim's system due to such cyberattack, but the perfect source of attack could not be traced or located. Therefore, healthy support to intrusion management process which tries to plug the security loop-holes may be found to be very helpful for the purpose of strengthening of the e-security.

The crucial cyberattack protection devices that may be used for the purpose of e-security may be provided into four important categories as,

1. Anti-virus software: computer scanning software is to be installed and used towards all points of the attack. All diskettes must be properly checked and scanned before being finally used on to network and to the attack servers.
2. Firewall settings: Firewall is a mostly default provided software which contains a layer of isolation lines between the inside system and the outside network. These technology of firewall has now been certified by the National Computer Security Association (NCSA).
3. Authentication: It indicates towards the protection of password so that only the appropriately authenticated users are allowed to get access to the specific network resource. The Bio-metric authentication device may also have used for the usage, wherein, the patterns arising out of a retinal optic lines of a person or the voice recognition etc. which are derived through the electronic analysis which support the user in order to make sure that whether such transmitted data is genuine or it is unauthorized.
4. Encryption: It mainly involves the swift variation of data into an indecipherable pattern prior to its transmission. Thus, even if it is transmitted, such data cannot

[290] Ravi B & akkanavar, *Causes of CyberCrime and Preventive Measures*, KRAZYTECH (2020), https://krazytech.com/technical-papers/cyber-crime (last visited Jul 26, 2020).

be properly interpreted. Such changed absurd data is also called as the cipher text. Encryption is to be accompanied by the decryption or by changing the unreadable text back towards its original form of data.[291]

The Data Protection:

The important right to privacy over the internet and the data protection have also been recognized as a basic human right by various international communities, India should provide an appropriate legislation in order to address such privacy and data related securities issues, so that a uniform pattern relating to the privacy standard is to be carried out by the netizens and the ISP's at various governmental as well as the non-governmental level. Towards this context, it may be highlighted that, though, the Article 21 provided in the Constitution of India[292] protects the right to privacy of an individual as a face of fundamental right, but it is present mainly and almost only against the state action and does not provides its protection against any actions of private parties. Section 72 of the Information Technology Act[293], also provides the security to the online data privacy over the computer, storage system device and the computer network, but it possesses only a limited scope. Therefore, the enforcement of an independent Online Data Protection Act which may be uniformly applicable to all the people, the organizations across the India as along the lines of the U.K. pattern may prove to be a walk forward towards the restriction and the control of any unlawful cyberattacks. The United Kingdom has its own special Data Protection Act 1998[294] in order to regulate data as well as any sensitive information processed through the computers or networks. Likewise, many countries like Germany, Austria and Scandinavia also possess their own electronic surveillance and information technology regulating laws in order to protect their data as well as the related personal data information.

[291] Systems Security: Firewalls, Encryption, Passwords & Biometrics - Video & Lesson Transcript, , STUDY.COM , https://study.com/academy/lesson/systems-security-firewalls-encryption-passwords-biometrics.html (last visited Jul 26, 2020).

[292] Article 21 of The Constitution of India - The Expanding Horizons, , http://www.legalserviceindia.com/articles/art222.htm (last visited Jul 26, 2020).

[293] Section 72: Breach of confidentiality and privacy - Information Tech. Law, *Supra* note 287.

[294] Data Protection Act - an overview | ScienceDirect Topics, , https://www.sciencedirect.com/topics/computer-science/data-protection-act (last visited Jul 26, 2020).

As an international effort for the protection of privacy and the transnational availability of the personal data, the Organisation for Economic Co-operation & Development (OECD) 1996[295]. It has issued guidelines consisting of certain basic principles with a view to attempting a balance between the protection of data privacy and the enhancement through the free flow of personal information throughout the various OECD countries. Thus, the personal data is secured by way of adopting the appropriate security safeguards against any form of risks of loss or for the unauthorized access, removal, destruction alteration, disclosure or use etc.

Shifting towards the Paperless Official Electronic Records:

In order to ensure the presence of a secured electronic information, agencies and organizations is to be made ensured that the appropriate electronic process collects all the relevant potential data and it is retained successfully and is always readily available. The reasonably long duration of time between the collection of such data information and its application in various areas and situations, such as, litigation, arbitration etc. which may be detrimental to the parties. It has also been pointed out that various agencies and organizations in India still retain pertinent portion of paper based documents in their first original form instead of transposing them into the electronic form as an authentic record. Also, the public of India, in general, place more trust and reliance upon the paper based documents rather than any form of electronic record.

While the process of such conversion of paper based record is in the electronic form, the proper care has to be taken such that legal rights of persons are not being disturbed and the veracity or the authenticity of such converted documents is not thwarted by any chance. As, it is the Government and the various organizations needs certain forms of transactions to be in physical and in the signed document form for their legal veracity. They also state that, the electronic records and signatures shall not be directly legally recognized. It is high time that, when this adversarial thinking is to be changed and it needs to be recognized that going the paperless by the switching towards the electronic record of documents is in no way reduces their legality. Since, the electronic records are readily

[295] OECD, , WIKIPEDIA (2020), https://en.wikipedia.org/w/index.php?title=OECD&oldid=968887334 (last visited Jul 26, 2020).

available and approachable, easy to contain and procure and almost always of a lasting nature, turning towards from paper based record towards the electronic paperless records would certainly foster the working and facilitate in boosting and accelerating the approach of cybercrime detection, investigation, inquiries and trial.[296]

Liability of ISP's requires reconsiderations:

It may be observed that, whenever a copyright holder charges action against any infringement on the internet, such owner invariably also sues the ISP as well along with such person, who actually commits that infringement. The intention of holding such ISP also contributorily liable for infringement is to compel him in order to delete such infringing material from his servers because he maintains that network. This fast growing trend by just targeting the ISP drags them towards the frequent litigation which pulls almost many of them towards closure of their negative internet services. Although, Section 79 of the IT Act[297] provides about the exemption from the liability to ISP under the two circumstances, mentioned as, i) When such person does not possess actual or any constructive knowledge about such illicit nature of such content they are providing over the internet. and; ii) Where they have appropriately conducted due diligence in order to avoid any contravention of law. But, such clause by itself, is just not enough and there is a significant need to classify ISPs as access providers, hosting service providers etc. as is already provided by the European countries. This may give a high moral motivation to the ISPs for willingly assisting the investigators towards the process of cybercrime identification and for the investigation and to infuse a sense of moral responsibility and moral consciousness among them to get the co-operate from the law enforcement bodies or agencies in order to crusade against any crime prevention.[298]

[296] Tyrustech, *Here's Why Top Indian Companies Are Switching To the Paperless Route – My Blog*, https://www.tyrustech.com/blog/heres-why-top-indian-companies-are-switching-to-the-paperless-route/ (last visited Jul 26, 2020).

[297] Section 79: Exemption from liability of intermediary in certain cases, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-79-exemption-from-liability-of-intermediary-in-certain-cases/ (last visited Jul 26, 2020).

[298] *Ibid.*

CHAPTER 7

INDIAN JUDICIAL APPROACH TOWARDS CYBER CRIMES

The fast growth in the cases of Cybercrimes incidents in India has created a new face of challenge for the Indian law enforcement agencies. The development of the Information Technology has placed real people beyond any form of physical boundaries to its entirety. The new digital global villages in India, which are coming into the existence with a serious rapid pace, are with the both, endless opportunities as well as the downsides.

The criminal justice society in India has achieved tremendous growth over a period of more than a century and has bagged international reputation as one of the most independent and effective judicial systems of the world. The integral agencies dealing with the administration of criminal justice mainly include the 'Parliament i.e., law-makers, the law enforcers, i.e., the prosecutors, lawyers and the judges'. They possess considerable functional legal independence yet their working has always been mainly based on the basic principle of checks and balances, which restricts them from encroaching upon each other's working domain as well as provides opportunity to act with complete co-ordination.[299]

7.1. JUDICIAL CHALLENGES AND CYBERCRIMES:

With the fast development of the computer software and the internet, online community has become an important part of the modern world growth as most of our sectors that is commerce, banking, exchange of money, industries, information communication, governmental and the non-governmental online transactions, academic research works etc. are carried on by the internet. The condition now is that whatever any person wants or wants to know about or want to see, he or she can access it through the internet. Despite this, the brighter side of this internet technology, there are certain negative sides which are of a sensitive cause of concern, not only for the Indian law-enforcement agencies but for the Indian judicial bodies as well. The internet communities in its wake, has given rise to a various number of online disputes, differences, controversies etc. resulting into the misuse of the potential information of the computer networks for the

[299] Criminal justice society of india | Breaking Stories and Opinion Articles, FIRSTPOST, https://www.firstpost.com/tag/criminal-justice-society-of-india (last visited Jul 27, 2020).

illegal activities. Although, the disputes as such are not new to human community, they are known to be present ever since the dawn of human civilization but the perturbing point is that the disputes which includes the online transactions are completely unique in their scope, nature and treatment and thus, the solution relating to these cyberspace related disputes has emerged as a serious challenge towards the courts of law because of the challenges involved in them with which the Judges are right now not thoroughly conversant.

The factors which adversely affect the process of the cybercrime cases are mentioned as:

1. The international nature of these cybercrimes are such that they do not recognize geographical areas or the territorial boundaries;
2. The variation in the legal regulations and laws and the procedure of various countries with regards to the admissibility of cyber space related cases; and,
3. Uncertainty, the appropriate definition of the cybercrime and activities which is to be included and to be covered within the ambit of 'cybercrime'.[300]

The problem of Cybercrime being of an intangible nature, it does not require any physical action or the physical presence of accused at the alleged scene of the crime. Under such circumstances, the traditional adversarial techniques relating to litigation would rarely meet the ends of justice in cases which mainly involves cybercrime. The dilemmas and issues faced by the Indian judiciary and the law enforcement agencies while dealing with the crimes related to the computer or cyberspace, the Hon'ble Supreme Court of India in the case of *State of Punjab and others v. M/s Amritsar Beverages Ltd. and others*[301], observed that:

"Internet and other related information technologies have tagged-up with them the problems which cannot been previously foreseen by law. Also, it did not foresee the upcoming difficulties which may be faced by the concerned officers who does not possess any scientific expertise or not have the sufficient knowledge to adjust with the new

[300] Cyber Criminals on Trial, , https://www.researchgate.net/publication/233023456_Cyber_Criminals_on_Trial (last visited Jul 26, 2020).
[301] State Of Punjab Vs. M/S. Amritsar Beverages Ltd., , https://www.legitquest.com/case/state-of-punjab-v-ms-amritsar-beverages-ltd/2ACA3 (last visited Jul 26, 2020).

situation. Numerous developments leading towards various forms of crimes which unforeseen by the Legislature came to immediate focus. The Information Technology Act, 2000, although, was altered time to time in order to include various forms of heinous cybercrimes and updated the appropriate punishments for them, but does not entirely deals with all problems which are encountered by the concerned officers enforcing such Act".[302]

7.2. NEW TRENDS IN JUDICIAL APPROACHES:

The main motive and the relevant circumstances under which such offence is being committed and its adverse effect on the victim and the society also has a bearing towards the sentencing of the accused. The offender's tender age, his immaturity and no previous criminal record are mostly positive grounds for the leniency towards sentencing while recidivism, continuous association with the criminals or criminal community is also attracts the quantum or the seriousness of crime also attracts the severe punishment.

Although, the case laws available on cybercrimes are by far scantier as compared to the other traditional crimes and these cases are constantly escalating due to the high usage of computer becoming more and more convenient and friendly with the people. The courts have shown a mentality to treat such cyber criminals guilty of the premeditated crime as significant danger to the society and therefore, they are ignorant towards mitigating the pronounced sentence of such offenders.

7.2.1. Trends in Indian Judicial System:

It must be duly mentioned that the Indian case law relating to the cyber jurisdiction of courts was almost absent until the special Information Technology Act, 2000 was enacted and was enforced on October 17, 2000. The enhancement of information technology as a faster and easier means of communication in these new millennium times has resulted to certain unforeseen consequences which ultimately resulting in the cybercrimes placing before the Courts for the adjudication.

[302] *Ibid.*

In the case of *P.R. Transport Agency v. Union of India and others*[303], it included the pertinent question relating to the jurisdiction of court, where the contract between the parties staying at different places has been agreed upon on e-mail. In this case, the Bharat Cooking Coal Ltd. (BCCL)[304] conducted an e-auction to sell-off coal in different lots in which plaintiff's i.e., P.R. Transport agency, gave bid for almost 40000 metric tons of coal from Dobari colliery was got accepted. The BCCL communicated the acceptance towards bid through e-mail on July 19, 2005. In response, the plaintiff deposited the appropriate amount 81.12 lakhs by providing a Cheque in favour of BCCL, they ultimately accepted the Cheque and encashed it, but did not gave the delivery of coal to the plaintiff. Instead, they (BCCL) informed the plaintiff by the e-mail that the said e-auction stands forfeited 'because of some technical, contingent and the unavoidable reasons'. The plaintiff came to know that, the e-auction for the sale of coal was ultimately cancelled by BCCL as there was any other person whose bid for coal was way higher, which was not been checked earlier because of certain glitch in the computer or in its program or in the feeding of data. The plaintiff i.e., P.R. Transport challenged such validity of cancellation of their contract by the defendant in the High Court of Allahabad. The defendant (BCCL) objected by questioning the territorial jurisdiction of the Hon'ble Court on the ground that, the High Court of Allahabad had no jurisdiction in the case as the cause of action, had not arisen in the state of Uttar Pradesh. The plaintiffs, on their part, argued that the case fell within the jurisdiction of the Court because the communication of acceptance of the tender was received by them through 'e-mail in Chandauli in U.P.', having heard both the parties, finally the High Court held that, in case of e-mail acceptance, the data transmitted from anywhere by the account-holder gets into the memory of 'server', which may be traced by anywhere and may be retrieved by such addressee account-holder from anywhere in the world. Therefore, there can be no fixed area, either for the transmission or in receipt of

[303] P. R. Transport Agency v Union of India (UOI) and others on 24 September 2005 - Judgement - LawyerServices, , https://www.lawyerservices.in/P-R-Transport-Agency-Versus-Union-of-India-UOI-and-others-2005-09-24 (last visited Jul 26, 2020).

[304] BCCL | Bharat Coking Coal Limited- A Subsidiary of Coal India Limited | A Govt. of India Undertaking | Dhanbad | Jharkhand | India - Bharat Coking Coal Limited -, , http://www.bcclweb.in/ (last visited Jul 26, 2020).

such e-mail. As it is stated in Section 13(3) of the Information Technology Act, 2000[305], "an electronic document is deemed to be received at the place where the addressee has his place of business. The acceptance of the tender will be deemed to be received by the plaintiff i.e., P.R. Transport at the place where they have head office for the business i.e. Varanasi and Chandauli and both comes in the state of Uttar Pradesh, therefore, the Allahabad High Court possess the sufficient jurisdiction for adjudging the case. In this case, on the basis of decision, it may be inferred that the judicial trend in relation to the exercise of jurisdiction by courts in cybercrimes must be in affirmation to the regulations of fair play and justice, which mainly depend on the following considerations:

A. the scope of the intentional intrusion or the illegal activities adversely affecting State's affairs;
B. the nature of conflict with the sovereignty of State;
C. the group of state's interest in the adjudication of the dispute;
D. State's responsibility for securing the interests of parties providing them solution; and
E. existence of an alternative groups.

In order to affirm the State's jurisdiction in the cyberspace, the law requires that it not only provides accessibility of the website but also in some way to communicate with the victim.[306]

7.2.2. Incidents of Child Pornography: Judicial Approach:

With the growing use of internet in the human life, there is predominant advent of the pornographic material on the web which has the adverse effect not only on minors and the young persons, but also on society as a whole. In common terms, the pornography may be said to be a predominantly, an obscene sexually explicit material that is intended, especially, for the purpose of sexual desire arousal.

[305] Section 13: Time and place of despatch and receipt of electronic record, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-13-time-and-place-of-despatch-and-receipt-of-electronic-record/ (last visited Jul 26, 2020).
[306] *Ibid.*

The main point behind rising cases of pornography as a cybercrime mainly appears to be that there is no regulation worth the name to limits or to regulate as to the type of persons, who are permitted to access the internet.

With regards the reported Indian cases on the cyber pornography, they are far and few as many of them are disposed of in the lower courts of India at the judicial level. Although, in the case of *State of Tamil Nadu v. Suhas Katti*[307], it deserves an important mention, in this context, since it was disposed of within a record period of seven months from the date of filing of such FIR. The credit for such excellent investigation relating to the case goes to the Cyber Crime Cell of Chennai which produced eighteen witnesses and the thirty-four documents in favour of the prosecution case. The facts of the case were as follows:

The accused i.e., Suhas Katti was publishing obscene, annoying and the defamatory messages relating to the complainant, a divorcee woman on e-mails and also in the Yahoo group. He had created a false e-mail account in the name of the victim. The e-mails carried a message that the victim lady was soliciting herself and therefore, she suddenly started receiving various disturbing phone calls from the callers to have sex. She filed FIR for such problem against the unknown accused in the Cyber Crime Cell, Chennai. The police investigation found out that the accused was a near family friend of the victim, who was staying in Mumbai and was actually interested in marrying her. She, however, married some another person with whom she divorced after sometime, so the accused again started contacting her for marriage with him, for which, she declined. Thereafter, he started harassing her by sending her obscene and defamatory e-mails.

The said accused was charged under Section 67 of the I.T. Act, 2000[308] read with Sections 469 and 509 of the Indian Penal Code. He pleaded that, such obscene e-mails might have been sent to the complainant either by her ex-husband, with whom she had divorced or might have managed to do so by herself to implicate the accused towards the case as he had turned down her proposal to marry her. On behalf of the accused, it was also

[307] State of Tamil Nadu Vs Suhas Katti - Cyber law case in India in Cyber laws, , FREE LEGAL ADVICE - LAWYERS FORUM, *Supra* note 277.

[308] Section 67 of Information Technology Act: Punishment for publishing or transmitting obscene material in electronic form, , INFORMATION TECH. LAW (2014), *Supra* note 272..

argued that, the provided documentary evidence against him are non-sustainable under Section 65(b) of the Indian Evidence Act[309]. The Court, although, relied upon the expert witnesses and other evidence before it including the witnesses such as owner of cyber cafe and convicted the accused for the offence under Sections 469,509 of Indian Penal Code[310] and Section 67 of the I.T. Act. The accused was sentenced for the charges of rigorous imprisonment for two years and charged with a fine for the offence under Section 469, and imprisonment for the term of one year along with a fine for the said offence committed under Section 509 of IPC and another sentence to undergo for a simple imprisonment of two years and along with a fine for an offence committed under Section 67 of the Information Technology Act. All the sentences were to be made to run concurrently.

In another famous case of *Avnish Bajaj v. State (NCT Delhi)*[311], Baazee.com was an e-auction website and Mr. Avnish Bajaj was the Chief Executive Officer (CEO) of the Company. He was charged and finally arrested in December, 2004 for transmitting the cyber pornographic material. The charges against him came from the fact that someone had sold the second of pornographic material CD through the Baazee.com website. The CD was also being found sold near the markets of Delhi. It was as an outcome of joint action of Delhi and Mumbai police that the accused was arrested. Although, Mr. Bajaj was later released on bail by the Delhi High Court as there was no prima facie evidence against him that proves that he was either directly or indirectly published the pornography material and the actual obscene recording of such chip could not be viewed on Baazee.com. The investigation in this case opened that, Bajaj was of an Indian origin and had his family ties in India. His company's web-site i.e. Baazee.com was actually a customer web-site which was mainly working with online sale of property on commission basis. Later, an obscene MMS clip of a DPS girl having fun was listed for sale on the website Baazee.com on November 27, 2004 and several copies of such clips were sold by the said company.

But, the accused i.e., Mr. Bajaj, in his defence, pleaded that Section 67 of the Information Technology Act under which he was charged and arrested relates to

[309] Vijayashankar Na, *Understanding Section 65B of Indian Evidence Act*, NAAVI (2020), https://www.naavi.org/wp/understanding-section-65b-of-indian-evidence-act/ (last visited Jul 26, 2020).
[310] Indian Penal Code, 1860 | Bare Acts | Law Library | AdvocateKhoj, , *Supra* note 242.
[311] Avnish Bajaj vs. State (N.C.T.) of Delhi (21.12.2004 - DELHC), , http://document.manupatra.com/delhi/2001-2004/dl2004/D041287.htm (last visited Jul 26, 2020).

publication of obscene material and not for the distribution of such material. Also, after come to know about such illegal nature of the disputed CD, he immediately initiated the steps to stop the sales of it within 38 hours, since the intervening period was a weekend. He also contended that the disputed obscene clip could not be viewed over the portals of Baazee.com and its sale relations were not routed through him.

The question for verdict in front the court for this case was to draw a demarcation between internet service provider and the content provider. The Court stated that, the burden lies on the accused to prove that he was playing only the role of service provider and not of the content provider. The Court finally held that, the accused deserved to be released on bail as the evidence provided that the obscene material may have been unwittingly offered to sale through his company's website and there was just fair probability of the alleged crime having been actually committed by any other person. The accused was, although, directed to furnish two sureties for one lakh rupees each and to surrender his passport and not to leave country without the due permission of the court.

It is pertinent to note that the High Court of Bombay in a suo motu *writ petition (No. 1611 of 2001)*[312] appointed a Committee for recommending the measures to protect and secure the minors from the pornographic and obscene material on the internet. Two activists, Jayesh and Sunil Thakkar wrote a letter to the Hon'ble Chief Justice of the Bombay High Court complaining relating to the creation and publication of pornographic sites on the internet.

The Division Bench of the Court presided over by the Chief Justice passed an order dated September 28, 2001[313], appointed a High Court Committee, for suggesting and recommending the ways, measures and medium to protect the minors from using the pornographic and obscene material on the internet. The Committee made different regulatory recommendations for the internet service providers (ISP), internet cafes and their appropriate licensing etc. It also recommended that, every visitor to the internet cafe be required to bring the photo ID card and suggested relative provisions for the protective

[312] Bombay High Court Special Committee Report : Shielding Minors From Cyberporn, , https://www.naavi.org/importantlaws/cyber_cafe/cover.htm (last visited Jul 26, 2020).
[313] *Ibid.*

software and emphasized the requirement for the co-ordination between ISP Association of India and CCIC[314].

7.2.3. IPR related Cybercrimes and Judicial Trends:

The judiciary has always relied upon to the needs of the diverse scenario with regard to the development of technologies. They have been used for its own interpretative principles to maintain a balance between the age-old orthodox laws with the advanced technological knowledge. Internet and various information technologies have brought with them various issues which were not foreseen earlier by the legal regime. The several new developments directing to the different forms of cybercrimes unforeseen by the Parliament have proceed to fore in the new millennium. with regards to the internet related IPR disputes arising as an outcome of development of computer world, the courts have played a role of a referee between such contesting litigants so as to confirm that injustice is not caused to anyone.

The concept of intellectual property mainly consists of a bundle of rights. Any sort of unlawful appropriation by which the owner is deprived completely or partially of his rights, is an offence punishable under Section 43 of the Information Technology Act, 2000[315]. Software piracy is a common form of IPR violation. Various other violations of IPR mainly includes infringement of copyright, trademark and the service mark violation, theft of network source code etc. The major case laws which highlights the judicial trend in India with regard to the online Intellectual Property violations and the relevant offences are hereby discussed as follows:

In *Kirloskar Diesel Reconstruction P. Ltd. v. Kirloskar Proprietary Ltd.*[316], the Bombay High Court, stated that the definition of the term 'trademark' includes within it the word 'mark', which indicates the name and thus, the mentioned term 'trademark'

[314] INTERNET SERVICE PROVIDERS ASSOCIATION OF INDIA, , http://www.ispai.in/UI/index.php (last visited Jul 26, 2020).

[315] Section 43 of Information Technology Act: Penalty and Compensation for damage to computer, , INFORMATION TECH. LAW (2014), *Supra* note 259.

[316] Bombay High Court Archives - Page 343 of 800, , FREE JUDGMENTS INDIA : LATEST SUPREME COURT AND HIGH COURT JUDGMENT , https://www.legalindia.com/judgments/category/high-court/bombay-high-court (last visited Jul 27, 2020).

provided in Section 105(c) of the Trademarks Act[317], is to be considered as a uniform comprehensive term including within it the ‘trade-name’ or the term ‘business-name’ and the name through which such article or goods are sold. Mainly, there must be a considerable balance between the mark used in relation to such goods and the claimant person claiming such right to the use of that mark. In the present case, the court restricted such defendant from using the trade name i.e., ‘Kirloskar’ for their major companies, as there was chances of likelihood of confusion or deception in front of the public which may resulting in the loses to the plaintiff. In other words, an act of passing off would lie in the cases of violation relating to trademark or trade-name. The defendant was, ultimately restrained from applying or using the name ‘kirloskar’ in their advertisements published online and internet related communications.

Analyzing the principles mentioning the law relating to the act of passing off, Hon’ble Justice A.P. Shah of the Bombay High Court, as he then was, referred to Lord Diplock's stated under the *Erven Warinick v. Townend* case[318], wherein, it was held that, the pertinent characteristics which needs to be mentioned for a valid passing off action are stated as:

1. Misrepresentation
2. done by any person during the course of normal trade or business,
3. to the existing customers of such goods or services provided by him,
4. which is evaluated in order to injure or damage the goodwill of any another trader as a foreseeable result; and,
5. which ultimately leads to actual damage towards the trade or goodwill of such trader through whom such action is brought against such defendant.

From the above stated characteristics, it is to be noted that the intent to deceive is not an essential requirement to prove the deception of the defendant. Although, it would not

[317] TRADE MARKS ACT, 1999, , http://ipindia.nic.in/writereaddata/Portal/ev/TM-ACT-1999.html#s104 (last visited Jul 27, 2020).

[318] ERVEN WARNINK B.V. AND ANOTHER v. J. TOWNEND & SONS (HULL) LTD. AND ANOTHER, , 97 RPC 31–106 (1980), https://academic.oup.com/rpc/article/97/2/31/1610174 (last visited Jul 27, 2020).

be wholly immaterial as it may help the court to draw inferences as to the motive of the defendant.[319]

The WIPO Administrative and Mediation Centre's decision in the case relating to arbitration of *Bennett Coleman &. Co. Ltd. v. Steven S. Lalvani*[320], along with another case, *Bennett Coleman & Co. Ltd. v. Long Distance Telephone Company*[321], provided the certain principles relating to cyber law mainly on domain name, which may provide effective guidelines for the prevention of cybersquatting and also the related crimes. The mentioned principles are:

1. Daily application of newspaper titles or marks in the hardcopy form or the electronic publication leads to a potential reputation which may not be allowed to hijacked relating to cyberspace by a squatter.
2. According to the principle of presumption, the time when anyone registers a domain name which has the trademark or any other mark of some other entity, it shall always be presumed that, the said person was fully realised of the existence of the said mark at the time when he applied towards such registration for the domain name.
3. The website being a 'postal address' to the other sites, it may be presumed that the defendant is being adopting the domain name to take benefit of the good reputation of the plaintiff's domain name.[322]

The facts of the case stated that, the complainant of Bennett Coleman & Co. Ltd. were the publishers of two reputed papers, titled as, "The Economic Times", which had an average daily circulation of circa 35 lakhs, and the "Times of India", which had a circulation of approximately 1.52 crores per day. Also, they were carrying out publication of various additional supplementary material using their brand name i.e., 'Times' and held

[319] *Ibid.*
[320] Bennett Coleman amp Co Ltd Vs Steven S Lalwani The Economic Times won the first | Course Hero, , https://www.coursehero.com/file/p3hadhq/Bennett-Coleman-amp-Co-Ltd-Vs-Steven-S-Lalwani-The-Economic-Times-won-the-first/ (last visited Jul 27, 2020).
[321] *Ibid.*
[322] *Ibid.*

domain names such as www.economictimes.com and www.timesofindia.com, applying them for their electronic publication of their respective afore mentioned two newspapers.

In India, the complainant had registered under the mark ‘The Economic Times’ mainly for newspapers, magazines, journals, books and other relevant literary works dated March 28, 1973 and the mark ‘The Times of India’ dated July 30, 1943.

The defendant i.e., Stevens S. Lalvani, a resident of Lipper Montclair, USA acquired the domain name ‘www.economictimes.com’ and registered it with the Network Solution (NSI)[323]. He also acquired the domain name of ‘www.thetimesofindia.com’ and registered it with the NSI for defendant’s Long Distance Telephone Co. having the exact same address. After that, Steven S. Lalvani and Long Distance Telephone Co., jointly built up the websites of two domain names with the consequence that any internet users who legitimately tries to go to the site of the Economic Times, when typed the same name in his browser is to be redirected to the host site of the defendant’s website and therefore became a cause for the great damage and harm to both of the mentioned reputed publications of the plaintiff i.e. Bennett Coleman & Co. Ltd. This situation was as it is, unabated until 1999 despite various notices and takes for negotiations with the defendants but the latter did not mend their ways and continued such awful activity which may be termed as cybersquatting.

During the near end of the 20th century, the practice of cybersquatting was a latest issue across the world because of the factor that the Network Solutions did not provide any norms for restriction on the registration of domain names. However, perturbed by this developing menace, the government of United States formed the Internet Corporation for Assigned Names and Numbers (ICANN)[324], which is now shaped as the international body which mainly works for observing, studying and managing the whole internet. ICANN has created a uniform Domain Name Dispute Resolution Policy[325] which finally came into effect from December, 1999.

[323] Network Solutions Inc, *Home*, https://www.nsi1.com (last visited Jul 27, 2020).

[324] ICANN, , https://www.icann.org/ (last visited Jul 27, 2020).

[325] Uniform Domain Name Dispute Resolution Policy - ICANN, , https://www.icann.org/resources/pages/policy-2012-02-25-en (last visited Jul 27, 2020).

Taking benefit of such Uniform Domain Name Dispute Resolution Policy, the complainant i.e., Bennett Coleman & Co. Ltd. filed two straight cases against the defendants in front of the WIPO Arbitration and Mediation Centre on dated 27 January, 2000. Both the complaints, being against the same defendants resulted in taken together and were boldly contested by the defendant i.e., Steven S. Lalvani. The case was decided by the body of WIPO Arbitration and Mediation Centre[326] ultimately in the favour of plaintiff and the defendant was made ordered to transfer both the disputed domain names to the respective name of the complainant.

7.2.4. Requirement of Cyber Forensics: Judicial View:

The term 'computer forensic' was coined and used for the first time by the International Association of Computer Specialists (IACS)[327] situated at Oregon (USA) in the year 1991. It is that branch of forensic science which is formed to trace and identify the domestic preserve of the extract digital information taken through the computer program to produce, preserve and store the evidence relating to the cybercrime before the respective court. The term 'computer forensic' is that branch of forensic science wherein the cybercrime investigation and critical analysis techniques are applied in order to determine the significant legal evidence in regards to a computer environment. Internet based forensics broadly cover three major sectors, such as (a) computer forensics (b) cyber forensics, and (c) software forensics[328].

Computer forensics mainly deals with the bundle of evidence extracted through the computer system media seized from the primary scene of crime by finding the hidden or removed information stored in the computer disk.

Cyber forensics may also be called as 'network forensics'[329], it is relating to the search and analysis of the collected digital or electronic evidence that is provided all across

[326] WIPO Arbitration and Mediation Center, , https://www.wipo.int/amc/en/center/background.html (last visited Jul 27, 2020).
[327] IACIS: International Association of Computer Investigative Specialists: Overview | LinkedIn, , https://www.linkedin.com/company/international-association-of-computer-investigative-specialists/ (last visited Jul 27, 2020).
[328] Computer Forensics, , https://www.edrm.net/glossary/computer-forensics/ (last visited Jul 27, 2020).
[329] Network Forensics - an overview | ScienceDirect Topics, , https://www.sciencedirect.com/topics/computer-science/network-forensics (last visited Jul 27, 2020).

the wide computer networks. The important object behind the cyber forensics is to discover the evidence and the assessment of the motive and actual identity of the perpetrator in order to determine the significant impact of criminal activity over the victims. This said methods aids to find out whether such pertinent information has been deleted, removed, modified or hidden deliberately, incidentally or intentionally with a view to causing damage to the victim. Software forensics deals with the author of the malicious code. The key to identify the creator of the suspect code is forming of the appropriate body of code.

In the case of *Firoz. v. State of Kerala*[330], where the Hon'ble court, inter-alia, stated that, the cyber forensics significantly helped the investigators of cybercrime to prove the intentions, mediums and opportunities for the criminal to commit the crime. As, it is the main purpose which prompted the perpetrator in order to commit the crime and methods adopted by him, such as, how, when and why it was done. The motive may be anything, from curiosity to money related attempts, revenge or misadventure.

As mentioned above, cyber forensics mainly revolve around the proceedings relating to the electronic records such as evidence in front of a court of law. The electronic records have been provided the legal recognition as under Section 4 of the Information Technology Act, 2000[331]. The substantial evidentiary value of a safe electronic record is more than any other form of electronic record as the burden of proof mainly lies on the person who claims damage or alteration in the electronic record. The electronic record bought before the court cannot ordinarily be substantiated through the written or tangible material or form of human witnesses. Therefore, it must be procured through the cyber forensics which includes analysis, discovery and reconstruction of evidence extracted from the system and/or contained in a computer, storage system, computer network, related media or computer peripheral.

Forensic assistance required for finding out the exactly which data was stored in a computer at such relevant time i.e. at the time of perpetration of cybercrime. There are various forms of information in a computer that are significant from the point of evidence,

[330] Firos vs State Of Kerala (2006), , INFORMATION TECH. LAW (2017), https://www.itlaw.in/firos-vs-state-of-kerala-2006/ (last visited Jul 27, 2020).

[331] Section 4: Legal Recognition of Electronic Records, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-4-legal-recognition-of-electronic-records/ (last visited Jul 27, 2020).

which can be traced or found out through the forensic procedure. The main among them includes normal storage files, removed files, hidden files, password protected information containing storage, data stored in free space, files slack, drive slack space etc.

The forensic technique of examination of data stored in a computer in order to ensure that the original evidence is not get tempered. This may be done by making the small images of the drives from the defendant's computers.

Pointing out the requirement and importance of cyber forensics in the investigation of cyber offences, the Court of United States in the case of *Easely McCaleb and Associates Inc. v. Perry*[332], stated that the deleted files on a defendant's system hard disk drive are discoverable and the forensic expert of plaintiff should be allowed to retrieve such recoverable files. In this case, the defendant through his own initiative had provided the hard disk drive in question relating to the court. The plaintiff applied for the discovery of its contents including the files that had been deleted, where they all could be recovered. The court granted the permission and provided an order for reviewing the electronically stored data of both the parties.

The Indian courts also recognize the fact that keeping the computerized record is rapidly becoming a normal procedure in the business and commercial world. Therefore, there is greater need to form the adequate forensic mechanism and to get the expertise in this field so that the investigation of cybercrimes is to be facilitated.

The computer related crime or any other related crime for that matter, requires various forms of evidence in order to make a small proof. Because of the intangible nature of large number of data kept in a computer which has multifarious roles, an essential technical cyber expertise is required which is a competent forensic expert can handle it properly. The intricacies involved under the investigation of computer related crime drew the attention over the investigating agencies and the courts in the Parliament Attack Case which happened at Delhi on December 13, 2001[333], wherein the court stated that the

[332] Dave Karpinsky, *Discovery of Electronic Evidence Allowable* 9 (2006).

[333] STATE (NCT OF DELHI) VS. NAVJOT SANDHU, , E-JUSTICE INDIA (2020), http://www.ejusticeindia.com/case-summary-state-nct-of-delhi-vs-navjot-sandhu/ (last visited Jul 29, 2020).

investigation of such crimes has to be provided to the specially trained experts investigating officials with the assistance of forensic experts, who have very deep knowledge relating to the working of computers and its related techniques.

7.2.5. Miscellaneous Cases Covered under Indian Judicial Trends:

The Hon'ble Supreme Court under *M/s Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd.*[334], has stated that, the domain name used as a medium of carrying on the commercial related activity has also possessed the characteristics of trademark. It cannot be considered as mere the address on internet but can be serves as a business identifier and thus, the passing off action may be charged for the violation of domain name related right.

In the another case of *State of Maharashtra v. Praful B. Desai*[335], the Hon'ble Supreme Court held that, the recording of evidence through the video conferencing in the presence of accused person is made permissible under Section 273 of the Code of Criminal Procedure, 1973. By precisely interpreting the phrase 'presence of the accused' used under this section, the court stated that the word 'presence' in the section does not mean the actual physical presence in the court, if the accused is even present on the computer or any video screen during the video conferencing, it will be as good evidence which is to be admissible similar to the actual humanely physical presence of the accused in the Indian court. The system of playback provides an additional arrangement in the cross-examination of witnesses. The recording system as an evidence through the video-conferencing considered to be more advantageous, wherein, witnesses cannot be procured without any undue delay, inconvenience or the expense.

In the present case, the wife of complainant was suffering from the problem of terminal cancer. The prosecution stated that the said lady was examined by Dr. Earnest Greenberg of Sloan Kettering Memorial Hospital at New York, United States, who had

[334] Satyam Infoway Ltd vs Siffynet Solutions Pvt. Ltd (2004), , INFORMATION TECH. LAW (2015), https://www.itlaw.in/satyam-infoway-ltd-vs-siffynet-solutions-pvt-ltd-2004/ (last visited Jul 27, 2020).

[335] The State Of Maharashtra vs Dr. Praful B. Desai, , https://www.indianemployees.com/judgments/details/the-state-of-maharashtra-vs-dr-praful-b-desai (last visited Jul 27, 2020).

opined that she was in the inoperable state and needs to be treated only with due medication.

The said respondent i.e., Dr. A.K. Mukherjee, who appeared for the charges under section 338 which is to be read along with sections 109 and 114, IPC, challenged the said validity of whole process against him but the Hon’ble Supreme Court instantly dismissed his special leave petition dated July 8, 1996 and provided direction to face such trail. On the date June 29, 1998, the prosecution also submitted the application in order to examine Dr. Greenberg through the video conferencing, which was finally allowed by the trial court dated August 16, 1999. Although, the respondent challenged that said order, therefore, the final appeal came in front of the Supreme Court. Dr. Greenberg had provided his due consent for giving evidence but he refused for coming to India for the said purpose. As, due to the absence of any provision compel him to appear as a witness to provide the evidence before Indian courts, the Apex Court provided the permission of the examination of Dr. Greenberg through the process of video-conferencing and rejected in the outset the plea of the respondents that, there was absence of provision for examination of witnesses through the video conferencing under the Code of Criminal Procedure and also, it could be made in contravention to the provisions of Section 273 of Cr. P.C.[336], which needs the actual physical presence of the witness in the Indian courts. The Court in this instant case stated that:

“The video conferencing is an advancement in the technology which ultimately allows one to see, observe, hear and talk with any other person far away through the same facility and with ease as if he is just present near to you. In fact, such person is present in front of you on a screen except available for touching, one can see, observe, listen and sense as if such person is present in the same room. In the medium of video conferencing both parties appear in presence of each other. Although, the evidence through the video conferencing should be on condition that such recording equipment have been set up inside

[336] CrPC Section 273 - Evidence to be taken in presence of accused, , A LAWYERS REFERENCE , https://devgan.in/crpc/section/273/ (last visited Jul 27, 2020).

the court itself so that such evidence can be recorded through the directions of the Magistrate."[337]

In the case of a foreign witness, such provided evidence through video-conferencing needs to be recorded by the court under the two conditions, such as,

(i) witness must be a legal national of a country which has signed an extradition treaty with India and under the said country's law of contempt of court; and

(ii) perjury should be considered as a punishable offence in that country. The completion of the said conditions may permit the court to exercise its jurisdiction in case, the foreign witness tends to or commits any contempt of court or in case perjures himself.[338]

7.2.6. E- Committee by the Supreme Court of India:

On the recommendation made by Justice R.C. Lahoti, the former Chief Justice of India, the Union Government finally appointed an e-committee dated on December 28, 2004 by the Chairmanship of Justice Dr. G.C. Bharuka, a former Judge of the Karnataka High Court along with three specialist members in the committee to prepare a National Policy for the computerization of justice delivery system in India to be implemented in a systematic phased manner.[339]

The established said e-committee released its report to the then Hon'ble Chief Justice of India Y.K Sabarwal dated November 5, 2005 after preparing consultations with legal and computer related experts and also internet service providers. The policy was proposed to be enforced in the three systematic phases during such ensuing five years.[340]

Moreover, the National e-Courts Project for extensively comprehensive computerization of courts was launched from the hands of Dr. A.P.J. Abdul Kalam, then

[337] The State Of Maharashtra vs Dr. Praful B. Desai, , https://www.indianemployees.com/judgments/details/the-state-of-maharashtra-vs-dr-praful-b-desai (last visited Jul 27, 2020).

[338] *Ibid.*

[339] Need for a uniformly enabled ICT for the Indian Judiciary, , https://www.barandbench.com/columns/need-for-an-ict-uniformly-enabled-indian-judiciary (last visited Jul 27, 2020).

[340] E-Committee | SUPREME COURT OF INDIA, , https://main.sci.gov.in/e-committee (last visited Jul 27, 2020).

President of India at New Delhi, along with the presence of Chief Justice of India, Law Minister of India and various other honorable dignitaries. The President of India highlighted his vision to create the e-Judiciary and the e-governance mechanism grid, by covering the entire Indian judicial system, which according to him, "will surely ensure the transparency, speed and balance in the decision making process".[341]

Currently, e-judiciary in India is at its operative stage in certain areas and informative stage various others, it will slowly enhance as the process of switch over to the programme of e-police stations and e-Courts gains significance in the upcoming years. Although, the pertinent issue relating to extra territorial jurisdiction of the courts over the criminals of cybercrime still remains under a grey area because of the high level variations in the criminal law and procedure prescribed by various countries. Also, the said issue is further complicated due to the anonymity of such criminals of internet related crimes and his actual physical non-existence at the scene or primary location of crime. These mentioned issues cannot be solved by any nation unilaterally, unless all the countries involved and affected by any connected case of cybercrime together and extend their sincere cooperation in catching such cyber criminals and to getting them punished.[342]

[341] e-Court Mission Mode Project/District Court in India | Official Website of District Court of India, , https://districts.ecourts.gov.in/nalanda/e-court-mission-mode-project (last visited Jul 27, 2020).
[342] *Ibid.*

CHAPTER 8

COMPARATIVE STUDY OF CYBER CRIMES

It is pertinent to note that various countries have adopted and updated their cyber laws in their respective legal systems in order to effectively deal with cyber related criminal activities. There are several countries who significantly updated the cyber laws in their countries while others have bought partial update in their domestic cyber laws. However, there are a number of countries which have not initiated measures for adoption of cyber laws to combat computer and cyberspace crimes. As the cybercrimes do not have any geographical or territorial boundaries, they are capable of breaching national borders which may cause serious threat to countries where legal protections against this crime are not adequate. Gaps and variations in domestic cyber laws of different nations renders prosecution of international cyber criminals uncertain.

At the outset, there are various forms of cybercrimes which the international community has highlighted to be of global nature. They may be described in the four broad categories as follows:

1. Data related cybercrimes, which covers the interception, modification and stealing of data;
2. Network related cybercrimes, which covers the interference and break down of network e.g. Distributed Denial of Service Attack (DDoS);
3. Crimes related to authorized access, such as, virus dissemination, hacking etc.; and
4. Computer related crimes which mainly covers the computer related fraud, forgery and aiding or abetting cyber criminals relating to e-commerce.[343]

Insufficient statutory protection of electronic information and weak legal enforcement mechanism for securing the network related information provides opportunity to the perpetrators of cybercrime to carry out their criminal activities on the internet across the borders being undeterred with least or negligible chances of being apprehended or to be nabbed.

[343] 17 Types of Cyber Attacks To Protect Against in 2020, , PHOENIXNAP GLOBAL IT SERVICES , https://phoenixnap.com/blog/?p=71548 (last visited Jul 27, 2020).

The level of growth made by the countries across the world in updating or altering their existing cyber related laws, according to UN report shows that, twenty-three percent of nations in the world already have significantly updated their cyber laws, while, some twenty-one percent have partially or have relatively less updated cyber laws and around fifty-six percent have not bought any changes in their cyber related laws as yet.

The cyber related legislation implemented by the United States, Australia, Japan and various other countries are discussed as model laws in relation to the cybercrimes and related laws, discussed as follows:

8.1. UNITED STATES OF AMERICA (USA):

The first federal computer related crime statute implemented in United States, was the Computer Fraud and Abuse Act, 1986[344] which was bought in order to reduce the problem of hacking of computers and related systems. It was further amended in the year 1994, 1996 and again in the year 2001 through the Patriot Act[345], which mainly deals with the new abuses arises out of the misuse of latest technologies. In United States of America, the States and the Federal Government have implemented the laws relating to cybercrimes. In States, the criminals of such cybercrimes are prosecuted under the statute nearly similar to the California's Penal Code[346] addressing the unauthorized access to the computers, computer systems or the computer networks. The mentioned statute deal with interfering, damaging, tempering or any unauthorized access to the computer system and computer networks. Also, the federal Government's computer crime statute, prohibits the unauthorized use of computer systems and alteration or the vanishing of records contained within them.

The United States Federal Criminal Code relating to the cybercrimes mentioned below as-

[344] Computer Fraud and Abuse Act - an overview | ScienceDirect Topics, , https://www.sciencedirect.com/topics/computer-science/computer-fraud-and-abuse-act (last visited Jul 27, 2020).

[345] USA PATRIOT Act | FinCEN.gov, , https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act (last visited Jul 27, 2020).

[346] California Penal Code, , http://individual.utoronto.ca/dubber/web/website/partIgen/California_Penal_Code.htm (last visited Jul 27, 2020).

1. fraud and related activity in connection with access devices,
2. fraud and related activity in connection with computers, and
3. communication lines, stations and systems.[347]

8.2. CANADA:

The Canada Criminal Code[348] mainly provides laws relating to unauthorized use of the computers and any illegal interception of communication as statutory offence which are made punishable under Section 342 and Section 184 of the Code respectively[349]. As a signatory member of the Council of Europe Convention on Cyber Crime, Canada[350] has implemented the cybercrime prohibitory law of the European Council with effect dated November 23, 2001.[351] The treaty which defining cybercrime includes the five broad areas of computer crimes, such as, unauthorized access of system, breach of the security and privacy related rights, violations of Intellectual Property Rights, offences against the classification and confidentiality and the computer related frauds.

Although, Canada has not been willing to ratify the European Council's Convention on cybercrime.[352]

8.3. UNITED KINGDOM:

The United Kingdom had duly implemented the Computer Misuse Act, 1990[353], although, due to certain further developments in the computer technology and subsequent emergence of latest cyberspace related crimes, further, new law against the cybercrime was introduced and implemented by the British Parliament which came into being with effect dated November 7, 2006. The law mainly targets and focuses on Denial of Service (DoS) attackers and provides punishment up to the period of ten years of imprisonment. It further

[347] 18 U.S. Code Part I - CRIMES, , LII / LEGAL INFORMATION INSTITUTE , https://www.law.cornell.edu/uscode/text/18/part-I (last visited Jul 27, 2020).
[348] Legislative Services Branch, *Consolidated federal laws of canada, Criminal Code* (2020), https://laws-lois.justice.gc.ca/eng/acts/c-46/ (last visited Jul 27, 2020).
[349] *Ibid.*
[350] Cybercrime: The Council of Europe Convention, , https://www.everycrsreport.com/reports/RS21208.html (last visited Jul 27, 2020).
[351] *Ibid.*
[352] *Ibid.*
[353] *Computer Misuse Act 1990*, https://www.legislation.gov.uk/ukpga/1990/18/contents (last visited Jul 27, 2020).

explains that, old Computer Misuse Act did not contain the main provisions relating to the DoS as an appropriate cyber offence, it only contained the penalties for modifying or changing the computer related data and its other contents without the authorization. The updated latest Act enumerates about the DoS attack as an unwanted act of flooding the server with huge quantities of irrelevant data until such server of the system crashes.[354]

According to the latest Computer Police & Justice Act, 2006[355], impairing or destroying the operation relating to any computer, restricting the access to any program or data to the computer and destroying the operation of any program on such computer are the crimes which are to be made punishable with the maximum period extended up to the ten years of imprisonment. Moreover, causing or forcefully making someone to do all or any of the above mentioned related crimes to be made punishable with the stringent imprisonment which may extend to the period up to two years.

Such stringent penal provisions provided in the Act almost always proved to be very effective in stopping the menace of DoS, which had a damaging effect on the internet users before the enactment of such new Act in the year 2006.[356]

8.4. AUSTRALIA:

Australia has been relatively steady while enforcing concerned legislation for cybercrime and had dynamic attempts and approaches across the various state territory and the federal jurisdictions. The Federal as well as the State Governments in Australia have finally enforced legislations forming different offences to control the issues relating to computer related crimes.

Under the Australian legal regime, a new Act called the “Cyber-crime Act, 2001”[357] was unveiled which came into effect on April 2, 2002 for amending the law with relation to computer related offences and also for other connected purposes. The mentioned Act

[354] *What is a Denial of Service (DoS) Attack?*, LIFARS, YOUR CYBER RESILIENCY PARTNER (2020), https://lifars.com/2020/03/what-is-a-denial-of-service-dos-attack/ (last visited Jul 27, 2020).
[355] *Police and Justice Act 2006,* https://www.legislation.gov.uk/ukpga/2006/48/part/5/crossheading/computer-misuse (last visited Jul 27, 2020).
[356] *Ibid.*
[357] AG, *Cybercrime Act 2001*, https://www.legislation.gov.au/Details/C2004A00937/Html/Text, http://www.legislation.gov.au/Details/C2004A00937 (last visited Jul 27, 2020).

provided a new Part 10.7 to the Criminal Code Act, 1995[358], such new part includes new computer related offences designed to address several types of cybercrime which damages or impairs the security, integrity, and reliability of computers' data and the electronic communications.

8.5. GERMANY:

The law governing and trying to secure the Internet and related electronic communications was enacted and enforced in Germany during 1970's[359]. Although, the Federation Data Protection Act, 1990[360] which was amended in September, 1994 was provided with a view to providing protection to individual against his right to privacy being damaged while handling his own personal data. This also enforced upon the public bodies of the Federation as also the private automatic data filing systems.

Moreover, Germany also applied the Telecommunications Act, 1997 which not only covered the protection relating to the specific copyright violations but it also provided certain liability for the online unlawful activities which holding the Internet Service Provider (ISP) invariably liable until such accused could prove that such person does not has the knowledge of such illegal content under the stored data.[361]

The Federation Data Protection Act, 1990 was further got replaced through the Federal Data Protection Act, 2002, which came into the effect from the January 1, 2002.[362]

Section 3 of the above mentioned Act mainly defines the data processing, while, Section 4 of the Act concerned with the admissibility of data processing and its related use. Also, Sections 5 and Section 6 of the Act mainly deals with the provision relating to the confidentiality of data as well as the inalienable rights relating to persons respectively.

[358] AG, *Criminal Code Act 1995*, https://www.legislation.gov.au/Details/C2017C00235/Html/Volume_1, http://www.legislation.gov.au/Details/C2017C00235 (last visited Jul 27, 2020).
[359] Edith Palmer, *Online Privacy Law: Germany | Law Library of Congress* (2012), https://www.loc.gov/law/help/online-privacy-law/2012/germany.php (last visited Jul 28, 2020).
[360] Federal Data Protection Act (BDSG), , https://www.gesetze-im-internet.de/englisch_bdsg/ (last visited Jul 28, 2020).
[361] *Telecommunications Act (Telekommunikationsgesetz, TKG) German Law Archive*, https://germanlawarchive.iuscomp.org/?p=692 (last visited Jul 28, 2020).
[362] Federal Data Protection Act (BDSG), *Supra* note 359.

Sections 7 and 8 of the said Act of 2002 also includes the provisions which mainly includes the schedule of compensation which is payable to public and also to the private bodies in case of illegal activities conducted in the violation of provisions of such Act.

Section 43 of the said Act mainly covers the offences and penalties under the Act. It provides that any person who without any authorization extracts, modifies, changes, retrieves or alters any potential personal data which is protected by the Act, shall be made liable with the imprisonment which may extend up to one year or with fine.

Sub-section (2) further enumerates that any person who illegally contains through any means of internet, network and any other medium of communication of personal data protected under this Act and all that are not known publicly, shall be made liable for the punishment up to the period of two years' imprisonment or with the fine.

Section 44 of the said Act mainly covers the administrative offences. It enumerates that the data can be taken from commonly accessible sources or from the Controller of such Data File, who possess the authority to publicize them. Although, if any person fails to comply with this provision, such person shall be made punishable with the fine which can extend to 5000 DM.

Recognizing concern for the emerging incidence of cybercrime cases in Germany, Gabriel Weidman, a Security expert of Germany, who is a professor at the University of Haifa in Israel and University of Maize situated at Germany has highlighted that there has been 40 per cent growth in the cybercrime rate. The main issue behind this growth was the use of high speed wireless Internet connections by such criminals of these crimes for deviating the investigators from the investigation and creating delusion among them so as to save themselves from detection and arrest. Weimann, therefore, implied that it was necessary to legalise online searches by amending the Federal Data Protection Act, 2002.[363]

Another cyber law expert Joerg Ziercke of German, pointed out that there are various terrorist groups who all are meeting regularly in the cyberspace through the internet and conducting their training camps and teachings online for instance, Al-Qaida has

[363] Cybersecurity: The backbone of a successful digital transformation, , https://english.bdi.eu/article/news/cybersecurity/ (last visited Jul 28, 2020).

launched their website that highlights how to use weapons, how to conduct the kidnapping and how to use herbs or fertilizers to create explosive bombs.[364]

8.6. FRANCE:

The laws of France in relation to Internet and the computer related crimes is mainly based on the European legislation which laid the foundation of legal statutes that formed and apply across the European country. The Parliament of Europe had enumerated the Council of European Directives in legal framework for the electronic signature and specific information services particularly the e-commerce on the December 13, 1999 which have been given effect by the France from June 8, 2000.[365]

With regards to the protection of Intellectual Property Rights over the Internet transactions, there is a French IP Code which secures the intellectual property rights to the creative works regardless of time, value, shape or purpose. France had enforced a legislation for regulating the electronic processing of such potential data. They provided a National Supervising Agency to regulate the implementation of this provided legislation. As far as domain name regime is concerned, the French Government has adopted the ICANN rules for the protection of domain names.[366]

8.7. SPAIN:

The Spanish Penal Code covers the computer related crimes such as unauthorized breach of the potential electronic mails or the information or its transfer, distribution and reproduction which is punishable with the imprisonment up to the four years. Article 248 of the said Code deals with computer related fraud and it is punishable with the imprisonment up to three years along with the fine.[367]

8.8. PHILIPPINES:

[364] Al Qaida ordered suspect to carry out attack in Germany - World - DAWN.COM, , https://www.dawn.com/news/625024 (last visited Jul 28, 2020).

[365] Council of Europe, , https://www.coe.int/en/web/portal/home (last visited Jul 28, 2020).

[366] Intellectual Property in France, , https://www.lawyersfrance.eu/intellectual-property-in-france (last visited Jul 28, 2020).

[367] Spain-Criminal Code (1995), , INTERNATIONAL COMMISSION OF JURISTS , https://www.icj.org/soginationallegislat/spain-criminal-code-1995/ (last visited Jul 28, 2020).

While the 'Love Bug' virus i.e., a worm[368], which travelled as an attachment as the e-mail messages of companies and individuals across the world, its genesis was located by the US Investigative Agencies along with the National Infrastructure Protection Centre (NIPC) at Philippines almost around 24 hours. They were able to trace the perpetrators with the important support of Philippines National Bureau of Investigation. Identifying that, the investigation in this case was influenced and hampered due to absence of appropriate computer crime law, the Philippines finally created and enacted a statute called the Philippines E-commerce Act, 2000.[369]

The creator behind the 'Love Bug' Virus, Onel de Guzmun, who was charged with the offence reported as fraud, malicious mischief, theft and violation of the newly enforced computer crime law. The Act may be considered as relatively effective in controlling and maintaining the incidences of internet related crimes at Philippines.[370]

8.9. SRI LANKA:

Sri Lanka, in order to curb the computer related crimes, finally enacted the Computer Crime Act, 2007[371], replacing its earlier Act. The crucial factor of the new Act is it primarily deals with the internet crimes such as hacking offences. It also enshrined provisions for expert penal to get the assistance to police for the Investigation of cybercrimes cases.

The Act criminalization policy attempts to target at the unauthorized access. It mainly discusses that any person who intentionally or without any legal authority carries out an activity which can potentially affect or damage any program relating to computer system or the Computer program, will be made liable for the crime which is to be made punishable under the Computer Crime Act.

[368] Love Bug's creator tracked down to repair shop in Manila - BBC News, , https://www.bbc.com/news/technology-52458765 (last visited Jul 28, 2020).

[369] The E-Commerce Law - Republic Act 8792, , DIGITALFILIPINO E-COMMERCE BOOT CAMP BY JANETTE TORAL , https://ecommercebootcamp.digitalfilipino.com/lesson/the-e-commerce-law/ (last visited Jul 28, 2020).

[370] Love Bug's creator tracked down to repair shop in Manila - BBC News, *Supra* note 367.

[371] Computer Crime Act | Volume II, , https://www.srilankalaw.lk/Volume-II/computer-crime-act.html (last visited Jul 28, 2020).

The Act also provides the expert panel with appropriate powers to be mentioned as, going at the scene of crime for the purposes of investigation and get access to examine the related system etc. It also discusses about the retention and restriction of the information needs to be availed from the computer devices in order to carrying out such investigation.[372]

According to the Information and Communication Technology Agency (ICTA) of Sri Lanka, internet related crimes mainly consist of three elements, such as, (i) computer related crimes, (ii) content related cybercrimes, and (iii) hacking offences.[373]

8.10. BANGLADESH:

The computer networks for the internet were established for the first time in 1964 at Bangladesh, although, the main frame installation had to be shut down in 1971 because of the outbreak of war with Pakistan following liberation movement in Bangladesh. It was, nonetheless, again restarted in the year 1975 after the complete independence of the Bangladesh.

The Government of Bangladesh formed and appointed an Expert Committee in June, 1997 to provide a legal framework for prevention and control of cybercrimes. The Committee submitted its report in the year 1999 in which approximately forty-five recommendations which were proposed for most of a comprehensive legislation relating to the cyber law. The Concerned Government affirmed the advice of certain changes and modifications in the proposed legislation, which were duly considered and advised by such Expert Committee, moreover, they also submitted its revised recommendations to the Government around the year 2002. Consequently, the Bangladesh Cyber Crime Act, 2004 came into the effect. The said Act enumerates the stringent and serious punishment towards the cyber offenders.[374]

8.11. PAKISTAN:

[372] *Ibid.*

[373] Information and Communication Technology Agency | ICTA, , ශ්‍රී ලංකා තොරතුරු හා සන්නිවේදන තාක්ෂණ නියෝජිතායතනය - ICTA , https://www.icta.lk/ (last visited Jul 28, 2020).

[374] CYBER CRIMES IN BANGLADESH, , THE LAWYERS & JURISTS , https://www.lawyersnjurists.com/article/cyber-crimes-bangladesh/ (last visited Jul 28, 2020).

Pakistan considered and applied the Prevention of Electronic Crimes Bill, 2007[375] enumerating the stringent punishments for those who indulge in stealing, destroying or illegally commercializing the potential information accessible at electronic networks. Moreover, in order to rectify certain deficiencies and lacunae relating to the Act, a proposed bill titled as, Cyber Crime (Prevention of Electronic Crimes) Bill was presented in front of the National Assembly in the year, 2007, but the said Bill bought several criticisms by the famous legal luminaries and was considered as an absurd and the draconian presented legislation which may make more harm than positive to the internet users.

Understanding and presenting the alleged drawbacks of such Bill, the famous Barrister of Pakistan, Zamid Jamal mentioned that, "Once this proposed legislation is promulgated by the National Assembly, innocent Pakistani people who have computer and use it on a day-to-day basis would be victim through its absurd effect as merely just retrieving or formatting a hard disk will bring a stringent punishment as seven years' imprisonment along with a fine of the amount ten lakh rupees."[376]

8.12. INTERNATIONAL BODIES CONCERNING E-COMMERCE:

In comparison to previous, several organizations have identified the organized cybercriminal networks as its most potential cyber security related threats and some are prepared to defend the said security threats. The facility of information technology is currently a double-edged sword, persistently providing us several advantages as well as disadvantages. The growing advent and opportunities relating to connections, developments, efficiency and effective communications across the world provides additional users under droves. The new method which has all of a sudden confronted the human society, but it does not differentiate between the good and bad, between national and international, between friend and enemy, between just and the unjust, but it only facilitates a medium for the activities which take place in the human society. Law as the

[375] Prevention Of Electronic Crimes Ordinance 2007 An Ordinance-Online Jounalism-Lecture Handouts - Docsity, , https://www.docsity.com/en/prevention-of-electronic-crimes-ordinance-2007-an-ordinance-online-jounalism-lecture-handouts/170656/ (last visited Jul 28, 2020).

[376] The Prevention of Electronic Crimes Act, 2016 (Act No. XL of 2016), http://nasirlawsite.com/laws/peca1.htm (last visited Jul 28, 2020).

guardian of the human behavior has made its entry into the world of cyberspace and is trying to maintain the balance from its manifold challenges.

Precaution and protection has long been merely a question of safety against the menace from the physical world. ‘cyberspace’ arose mainly in the late last centuries. This new world is growingly the intertwined along with the traditional offline world, therefore, the protection under cyberspace has become a prerequisite towards a well-functioning society.

There are various international agencies which works to provide regulations for trade and e-commerce at the international level and facilitate with a forum for the purpose of providing resolution for the disputes and issues through the mutual negotiations. The important among them are as follows:

8.12.1. World Trade Organization (WTO):

It was during the ending of World War II (1939-45) that the various finance related experts and economists around the world came together at Briton Woods, Hampshire and provided their suggestions after careful study for the setting up of the comprehensive international agency in order to fix and restore the current economic order for harmonizing the tariff and the related international trade and in order to fix various monetary related issues. Initially, there was general proposal for setting up an International Trade Organisation but finally it could not come into reality because of the opposition by the US Congress. Although, the member representatives of fifty-six countries came together again in Havana in the year 1947 to create certain standard guidelines in order to improve, uniforms and regulates the International Trade. Therefore, finally, General Agreement on Tariff and Trade (GATT)[377] was created and signed by the contracting member countries finally in December 1947. Generally, GATT dealt with the process of deducing the tariffs and enhancing the efficiency of trade across the various nations, but there was no any dispute resolution mechanism covered under it.[378]

[377] General Agreement on Tariffs and Trade | international relations | Britannica, , https://www.britannica.com/topic/General-Agreement-on-Tariffs-and-Trade (last visited Jul 29, 2020).
[378] *Ibid.*

The eighth round of General Agreement of Tariff and Trade was held in Uruguay in the year 1986, provided with the proposal for the purpose of creating the World Trade Organisation (WTO) which mainly was proposed to face with the following issues:

1. Trade aspects relating to the intellectual property rights.
2. Various measures relating to cross-investment.
3. Trade relating to the service sector.
4. Measures relating to agriculture subsidy;
5. Dispute resolution mechanisms relating to trade;[379]

Therefore, GATT mostly tent to be active nearly for five decades. Thus, the final draft designed and prepared by Author Dunkel, the then Secretary-General of the Board of Trade was finally accepted and approved and formally signed on April 15, 1994 by almost one hundred and twenty-five Countries in the meeting held at Morocco and finally, it was accepted by all that the World Trade Organisation (WTO) be established from January 1, 1995 to work as a trade policy reviewing organ and a trade related dispute resolution forum. Moreover, various agreements, such as, an agreement relating to the Trade Related aspect of Intellectual Property Rights (TRIPS)[380] which was also ratified by the present member countries for the safety of computer software and its related copyrights.

The World Trade Organisation (WTO) being a successor to the GATT, is an International Organisation designed to supervise and liberalize the International Trade. It mainly covers the rules and regulations relating to the trade between nations at the global level and is created mainly for negotiating and implementing the new trade related agreements and tend to secure the member country's minimum adherence towards almost all the WTO provided agreements and the related ratification to be done by the respective governments in their domestic laws.[381]

Such member countries to be considered obliged to follow by such articles of the Berne convention which includes minimum standard which is to be met and the member

[379] World Trade Organization - Global trade, , https://www.wto.org/index.htm (last visited Jul 28, 2020).
[380] TRIPS Agreement, , WIKIPEDIA (2020), https://en.wikipedia.org/w/index.php?title=TRIPS_Agreement&oldid=962253837 (last visited Jul 28, 2020).
[381] World Trade Organization - Global trade, *Supra* note 378.

countries are free to enhance their respective Intellectual Property regimes. The mentioned Berne Convention enumerated and applicable for the minimum protection of literary and artistic work i.e., Copyright through an international agreement across the member states.[382]

The United States Commission on International Trade Law (UNCITRAL) was formed through the United Nations resolution in 1976 with a target for harmonizing the International Trade Law. The law for the e-commerce was finally resolved to be applied by the General Assembly through its resolution on the January 13, 2007, which has provided the access to the International Trade among various Countries through the e-commerce to a very reasonable extent.[383]

8.12.2. WIPO Copyright Treaty, 1996:

The creation of the World Intellectual Property Organisation (WIPO) can be traced back in the year 1883, when the Paris Convention for protection of Industrial Property was conducted and finally a treaty was finalized and ratified for the protection of intellectual creations such as patents. After that, the copyright got space into the International Arena through the Berne Convention (1971) for the protection of Copyright. In 1974, WIPO became a specialized agency under the United Nations with an authority to administer the intellectual property related matters.

In the year 1996, the World Intellectual Property Organisation (WIPO) formalized two treaties commonly termed as Internet Treaties for Countering the Challenges caused by the Internet Crimes. Although, the treaties are still silent on the area of liberty for the Internet Service Providers, as the problems relating to the liability has been left for the national legislations for the purpose of determination. [384]

The WIPO copyright treaty which was ultimately finalized in Geneva on December 20, 1996, and came into effect from 2002, highlighted about the right relating to

[382] Berne Convention | copyright law | Britannica, , https://www.britannica.com/topic/Berne-Convention (last visited Jul 28, 2020).

[383] United Nations Commission On International Trade Law |, , https://uncitral.un.org/ (last visited Jul 28, 2020).

[384] WIPO - World Intellectual Property Organization, , https://www.wipo.int/portal/en/index.html (last visited Jul 28, 2020).

communication but does not possess a provision relating to the right of reproduction. It only clarifies with that digital copies will also be considered as the reproduction with relation to the copyright law. Nonetheless, the various problems pertaining to the Intellectual Property Rights Violations over the internet have been included under the WIPO Copyright Treaty, the member countries are free to enhance their own Intellectual Property regulations and statutes.[385]

8.12.3. Internet Corporation for Assigned Names and Numbers (ICANN):

The domain name related disputes are being resolved mainly through the online arbitration under the Uniform Domain Name Disputes Resolution Policy finally been formulated by the ICANN which has headquarter in the California. It was formed on the September 18, 1998 in order to maintain various related tasks such as managing the assignment relating to the domain names and the IP addresses.[386]

The disputes relating to the domain name are settled through the Approved Dispute Resolution Service Providers (ADRSP). It exercises its control across the entire Internet and Thus, dealing with the hardships or the citizens and duly recognize the sovereignty towards the prevalent legal systems across different nations.[387]

8.13. BRIEF OVERVIEW OF INFORMATION TECHNOLOGY ACT, 2000, INDIA:

Section 1 & Section 2 of Information Technology Act is titled ‘Preliminary’. Section 1 covers the provisions relating to the short title, the commencement and its application. Under Section 2 several pertinent definitions have been provided.[388]

The Information Technology Act named the “Digital Signature and the Electronic Signature, and contains section 3 and 3A and particularly stipulates that, any subscriber may authenticate the electronic record by affixing the digital signature and the electronic

[385] WIPO Copyright Treaty (WCT), , https://www.wipo.int/treaties/en/ip/wct/index.html (last visited Jul 28, 2020).

[386] ICANN, , https://www.icann.org/ (last visited Jul 27, 2020).

[387] Approved Dispute Resolution Service Providers - ICANN, , https://www.icann.org/resources/pages/providers-6d-2012-02-25-en (last visited Jul 28, 2020).

[388] Chapter 1: Preliminary, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/chapter-1-preliminary/ (last visited Jul 28, 2020).

signature. It further enumerates that anyone can audit an electronic record by the application of a public key of the subscriber.[389]

Section 4 to 10A of the said Information Technology Act is titled as "Electronic Governance". It is mainly about the Electronic Governance and contains the inter alia amongst others that where any law enumerates that the information or any other related content shall be made in writing or to be the typewritten or in the printed form, then, notwithstanding, anything contained in the provided law, such mentioned demands shall be deemed to have been fulfilled if such information or related matter is rendered or made available in an electronic form and been accessible so as to be beneficial for a subsequent reference. This chapter is in connection with the legal recognition relating to the electronic record and the Digital Signatures, their application in the Government, for the foster delivery of services to the people through the electronic mediums, retention of any electronic records, publication under the Electronic Gazette and also provided to the Central Government in order to frame rules with respect to the digital signatures.[390]

Sections 11 to 13 of the said Information Technology Act deals with the "Attribution, Acknowledgment and Dispatch of Electronic Records". These sections mainly focus towards the attribution relating to electronic records, acknowledgment of such receipt, duration and related place of dispatch and such receipt of the electronic record.[391]

The mentioned Information Technology Act titled "Secure Electronic Records and Secure Electronic Signatures" which is included under the sections 14 to 16. These Section enumerates provisions in order to secure the electronic record, secure the relevant electronic signatures and related security procedure.[392]

[389] Chapter 2: Digital Signature and Electronic Signature, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/chapter-2-digital-signature-and-electronic-signature/ (last visited Jul 28, 2020).

[390] Chapter 3: Electronic Governance, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/chapter-3-electronic-governance/ (last visited Jul 28, 2020).

[391] Chapter 4: Attribution Acknowledgment and Dispatch of Electronic Records, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/chapter-4-attribution-acknowledgment-and-dispatch-of-electronic-records/ (last visited Jul 28, 2020).

[392] Chapter 5: Secure Electronic Records And Secure Electronic Signatures, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/chapter-5-secure-electronic-records-and-secure-electronic-signatures/ (last visited Jul 28, 2020).

The Information Technology Act contains the "Regulation of Certifying Authority" which mainly covered under Section 17-34. It provides a comprehensive scheme towards the Regulation of Certifying Authorities. The Act envisages a Controller as a Certifying Authorities, who shall mainly perform the activities relating to exercising the supervision over such related activities, the Certifying Authorities also provided the specific standards and conditions for the purpose of governing such Certifying Authorities as also specifying the several types and content relating to the Digital Signature Certificates. The said Act also recognizes the requirement for identifying the Foreign Certifying Authorities and Moreover, it also enumerates several provisions in relation to the issue of license and to issue the Digital Signature Certificates.[393]

The "Electronic Signature Certificates" mainly provided under section 35 to 39. These sections furthermore enumerate relating to the scheme of various conditions relating to representation, revocation, suspension of the Electronic Signature Certificates.[394]

The Information Technology Art provides the "Duties of Subscriber" enumerated under Section 40 to 42. This chapter contains discussion in relation to generating the key pairs i.e., public key and private key, duties for subscriber towards the electronic signature certificate, acceptance of such digital signature certificate and proper control relating to private key.[395]

The said Act provided "Penalties, Compensation and Adjunction" mentioned under Sections 43 to 47. This Chapter discusses in relation to the penalties and adjudication towards several Offences. The penalties relating to the damage towards computer, internet etc., has been provided as a way of damages through the specified compensation to such victim or affected persons. It also contains the compensation not exceeding the amount of Five Crore Rupees, towards the person so affected through such failure to protect the date. The said Act also includes the appointment of any officers not below the provided rank of a Director for the Government of India or any of the equivalent officer for state government

[393] Chapter 6: Regulation Of Certifying Authorities, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/chapter-6-regulation-of-certifying-authorities/ (last visited Jul 28, 2020).
[394] Chapter 7: Electronic Signature Certificates, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/chapter-7-electronic-signature-certificates/ (last visited Jul 28, 2020).
[395] Chapter 8: Duties-of-subscribers, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/chapter-8-duties-of-subscribers/ (last visited Jul 28, 2020).

as an Adjudicating Officer, who shall mainly adjudicate that whether any person works in the contravention of any above mentioned provisions of the said Act or the provided rules framed thereunder. The said Adjudicating Officer has been provided with the powers resembling to a Civil Court.[396]

From Section 48 to 64 of the mentioned Act named as "The Cyber Appellate Tribunal". It mainly covers the establishment of the "Cyber Appellate Tribunal (CAT)", which shall be an appellate body where appeals held against any orders passed by the concerned Adjudicating Officers shall be preferred. Moreover, this chapter also provides the issues pertaining to the legal representation, conditions, jurisdiction of the civil courts, appeal to the High Court, compounding nature through contraventions and the recovery of the penalty. This chapter also provides alongside the Composition of Cyber Appellate Tribunal, Qualifications relating to the Appointment as a Chairperson and Members of such Cyber Appellate Tribunal, Tenure of the Office, Allowances and Salary, various Conditions of Service, etc. of Chairperson and Members; Powers possessed through Superintendence, general direction, Powers of the Chairperson for the transfer cases, Decision taken by the majority, for filling up the vacancies and the Resignation and removal etc.[397]

The Offences which mentioned under Section 65 to 78 of the said Act, discusses mainly about several Offences and provides that such said offences shall be investigated only by the Police Officer who is not below the rank of the Inspector. Such Offences broadly covers the tampering of the computer source documents, any computer related offences, sending and transmitting any offensive messages through the computer communication service etc., publishing or transmitting any obscene material in the electronic form through the electronic medium, publishing or transmitting any material which is sexually explicit, not obeying and disrespecting the Controller's Orders and the directions, securing or attempting to get the access into the protected system etc. Moreover, this chapter also includes the problems relating to extra-territorial jurisdiction provided

[396] Chapter 9: Penalties Compensation And Adjudication, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/chapter-9-penalties-compensation-and-adjudication/ (last visited Jul 28, 2020).

[397] Chapter 10: The Cyber Appellate Tribunal, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/chapter-10-the-cyber-appellate-tribunal/ (last visited Jul 28, 2020).

under the Act, also the confiscation and investigation relating to offences. This chapter provides that the Central Government possess Power to issue guidelines for blocking the public access relating to any information through any related computer resource, to provide authorization to monitor and collect the traffic data or the information from any computer resource for the purpose of Cyber Security and also Central Government may designate any organization works under the Government as the national nodal body with respect to the Critical Information Infrastructure Protection.[398]

Section 79 includes the Chapter "Intermediaries Not to Be Liable in Certain Cases." Which enumerates that the intermediary (Network Service Provider) shall not be made liable towards any third party information, data, or any link for communication provided through such intermediary.[399]

The Chapter under the said Act titled "Examiner of Electronic Evidence" contained under Section 79A, which provides that the Central Government may notify for an Examiner of Electronic Evidence in order to provide the expert opinion over the electronic form evidence in front of any court or any other concerned authority.[400]

The Chapter under the concerned Act titled "Miscellaneous" provided under Sections 80 to 94. This chapter mainly covers the power of the Police Officer and other concerned Officers to enter, for search, etc. nature of Overriding effects of the Information Technology Act, application of the Act in the cases relating to electronic Cheque, truncated Cheque, Public Servant, Protection of Action taken in Good Faith, prescribe the areas or the methods for the encryption, punishment towards the abetment and the attempt to the commit, offences relating to Companies and also the Removal of difficulties. It also includes the formation of the Cyber Regulations Advisory Committee, which shall time-to-time advices the government as regards any related rules or for any other related purpose concerned with the said Act. This chapter actually empowers the Central Government,

[398] Chapter 11: Offences - Information Technology Act, *Supra* note 286.

[399] Chapter 12: Intermediaries Not To Be Liable In Certain Cases, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/chapter-12-intermediaries-not-to-be-liable-in-certain-cases/ (last visited Jul 28, 2020).

[400] Chapter 12A: Examiner Of Electronic Evidence, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/chapter-12a-examiner-of-electronic-evidence/ (last visited Jul 28, 2020).

State Government and the Controller in order to make certain rules, regulations or guidelines relating to Information Technology.[401]

[401] Chapter 13: Miscellaneous, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/chapter-13-miscellaneous/ (last visited Jul 28, 2020).

CHAPTER 9

CRITICAL ANALYSES OF DATA COLLECTED

"Everything has been said already, but as no one listens, we must always begin again."

- Andre Gide,
French Philosopher

9.1. THE FORENSICS:

The forensics measures can be taken only after the crime scene is procured from any harm to anyone at such scene. Securing such crime scene is really not that distinct with the internet related crimes than it is with adversarial, non-internet crimes. It is pertinent in securing the officer's protection, the protection for the bystanders, and the victim's protection and welfare. In certain cases, the first responders may not be experts in the computer forensics and might focus instead more on the non-computer related aspects relating to the crime. Many times, the first responder in the crime scene may unable to observe at the complete forms of crime that may have occurred. Such mentioned first responder may generally more engrossed in direct and physical dangers.

First and most importantly, the overall boundaries of the crime scene need to be observed. There is usually an inner periphery, the spot the crime occurred and the protracted perimeter. The core edge is where the actual crime occurred, and the protracted perimeter would be the surrounding zone where the criminal may have visited or exited the crime scene or unknowingly left out some clues that need to be recorded. Creating and controlling that boundary is crucial in maintaining the chain of evidence and confirming that the potential evidence is collected.[402] There are three major steps involved in starting of any forensic investigation, including the computer forensics:

1. Procure the Crime Scene;
2. Eliminate individual involved; and
3. Record all the activity.

[402] Forensic science, , ENCYCLOPEDIA BRITANNICA , https://www.britannica.com/science/forensic-science (last visited Jul 28, 2020).

9.1.1. Procuring the Crime Scene:

In an adversarial crime, for instance, a robbery or a murder, the outline of such area is usually marked with police seals or police barriers. The police seal or covered area itself is just to highlight all the parties of where such perimeter lies for the crime scene. It point-out the area that must be secured. Procuring such area includes a number of steps. First and foremost, remove any unnecessary persons from such crime scene. The rule is practical: If any person does not absolutely deserve to be there, such person should not be, and that also covers the other law enforcement personnel. Unwanted people at that crime scene may bring the opportunities towards the potential evidence to be compromised.[403]

Moreover, it is crucial to highlight the whole area, completely isolate the crime scene and prevent unnecessary people from getting into the crime scene. It is important to note that, the more people under the crime scene, there is a high need to clarify why they were present in the crime scene. Every entered person in the crime scene could leave some kind of trace which may dilute some potential evidence, for instance, hair, clothing thread part, or any other such contaminants. Making the travel traffic to be very less by just permitting only the essential personnel into the scene. Such personnel are liable towards their activities under the crime scene and whatever they record along with their addition to the initial report. Also, there are certain police personnel, keeping full record of who comes and exits the scene. That maintained record is so very crucial. The attorneys for defence may try to prove that such crime scene was contaminated due to the presence of different people in such crime scene who were not relevant. Such process may also be taken very resembling with a computer related crime.[404]

Apparently, procuring any computer related crime scene may be way different from procuring a traditional crime scene. The actual crime scene in the computer related crime is basically the actual computers, networks, wires, and servers related to such crime. In order to procure them, they must be taken physically and offline. If there is a computer or system which is suspected of being the main asset for committing a crime i.e., a tool used

[403] Forensic investigation of the crime scene, CEPOL (2014), https://www.cepol.europa.eu/media/blog/forensic-investigation-crime-scene (last visited Jul 28, 2020).
[404] JOHN R. VACCA, COMPUTER FORENSICS: COMPUTER CRIME SCENE INVESTIGATION (2008).

by the criminal, then such instrument too must be procured. There is where the computer related crime conflicts with the traditional crimes, defining the overall area of the crime. The several machineries may be geographically differentiated from each other, but it is still just as important that they are protected and properly isolated so that they can be carefully examined. Minimize the ratio of people who get access to the crime scene and to record all the interactions with the scene that is, the servers, workstations, routers, logs, or other areas of the crime scene. In several cases, the computer or systems indulged may be needed for the victim's operations to continue. For instance, if a company's server relating to its database has been hacked and such potential data breached or stolen, they will still require such server in order to continue operating business. The technique then, may be to obtain the server offline temporarily, duplicate the hard drives from the company's server and just get such duplicate drives into the service back, thereby, keeping the original drive protected as a potential evidence.[405]

9.1.2. Eliminating the Individuals involved:

In the criminal investigation, the witnesses and suspects, who were present at the scene should be removed and placed in different holding areas. It may risk whole investigation to leave the witnesses or suspects together with each other and also unattended. Reasonably isolating such parties' mays protect the genuineness of traditional and electronic evidence that is to be procured. Also, this resemble in the case of investigating the computer related crimes. Similar to any other crime scene, any person who in any case does not deserve to be present at the scene should not be there. Only those important personnel required towards the investigation to be provided the access to the area which involves the computer equipment, and each and every occurrence of that access must be recorded.

The suspected people related to the crime must be separated from any such computer equipment involved in the crime. This prevents the suspects from eliminating any potential evidence, and it also prevents all the related parties from accidentally altering or destroying evidence. It is important to note that in any civil or criminal trial, balancing

[405] *Ibid.*

the chain of custody is to be a crucial factor. Any problems relating to the chain of custody will give chance to the opposing counsel to question the admissibility of such evidence. There are several bodies or agencies that will provide assistance to people in the search for and gathering of evidence, especially, if not done before. There is also chance to equip the non–legal-enforcement consultants that can provide best possible assistance in computer forensics, for instance, computer-science professors or any other experts in computer forensics who are willing to provide assistance.[406]

9.1.3. Record all the Activity:

The crucial part of investigation is appropriate records of the relevant evidence. Any imbalance in properly documenting the evidence may make it inadmissible. The first step in recording the evidence is to closely observe the crime scene especially, any electronic evidence and be always alert that such scene relating to a computer related crime may not be like any other crime scenes. Any evidence recorded must be handled properly. Evidence tags are important to highlight the evidence. In the present internet age, there are several types of electronic or internet enabled devices that perpetrators can use to store evidence. It’s not just the system and its hard drives that needs to be looked but also for other devices such as, Pen drives, USBs, Cell phones, Memory cards, floppy, etc.[407]

9.2. PROCURING EVIDENCE FROM HARDWARE:

There are several tools available that one can use to collect the evidence from the hard-drive. Although, it is essential for any investigator to be aware about his or her options while opting any forensic tools. Whatever tool is selected; it should have capabilities to be sufficed in front of court cases.[408]

9.2.1. Access Data Forensic Toolkit:

[406] ROLE AND IMPACT OF DIGITAL FORENSICS IN CYBER CRIME INVESTIGATIONS, , https://www.researchgate.net/publication/331991596_ROLE_AND_IMPACT_OF_DIGITAL_FORENSICS_IN_CYBER_CRIME_INVESTIGATIONS (last visited Jul 28, 2020).

[407] 5 Steps for Conducting Computer Forensics Investigations | Norwich University Online, , https://online.norwich.edu/academic-programs/resources/5-steps-for-conducting-computer-forensics-investigations (last visited Jul 28, 2020).

[408] *Ibid.*

A company called AccessData Corporation founded in the year 1987, pioneered digital investigation by creating the FTK (Forensic Toolkit) for the purpose of computer related forensics. It has the professional capacity to provide the analysis, decryption, and breaking the password all within an informative, customizable, and have user-friendly interface. Two very crucial features of this tool are its ability to closely analyze the Windows Registry and its capability to crack the strongest passwords. The Windows Registry is where the Windows feeds all the important information regarding any installed programs, including worms, viruses, Trojan horses, hidden dangerous programs and spyware. The ability efficiently scanning and collecting data of the Registry to present it as evidence is important, and the ability to break the passwords for common applications is also crucial. The potential evidence can be stored in a strong password-protected file of Adobe PDF, Excel spreadsheet, or any other relevant application. This AccessData FTK possess the capability to crack passwords over more than 100 common frequently used applications.

Moreover, another very important feature of this asset is its capability of distributed processing. Scanning the complete hard drive, tracing the host Registry, and performing a critical forensic analysis of a computer could be a very tedious and time-intensive task. But through the AccessData's Forensic Toolkit, such multi-processing, tracing and analytics work can be divided across up to the level of three computers. This allows all three computers process the analysis in parallel, therefore, relatively speeding up the whole forensic process.

This toolkit is also available for Macintosh systems. Many commercial products are only available for Windows, and the open-source community usually focuses on Unix and Linux, so the Macintosh compatibility increases its value significantly. Also, this toolkit equipped with an Explicit Image Detection add-on which in few minutes automatically detects the pornographic images, which plays very significant role towards the allegations relating to child pornography.[409]

9.2.2. E-fense Helix:

[409] Forensic Toolkit (FTK)®, , ACCESSDATA , https://accessdata.com/products-services/forensic-toolkit-ftk (last visited Jul 28, 2020).

E-fense Helix found into a customized Linux environment and covers several applications structured for the incident response and for the forensics of Unix, Linux, and Windows machines. This tool has been critically designed to not touch the host computer in any way, in order to maintaining the computer forensically clean and sound. This is pertinent for any forensic tool. If, at the time of an investigation, the tool traces modified files in any way, the evidence becomes non-sustainable.

In addition to analyzing the hard drives, this tool can possess the live sensitive evidence through RAM or through any USB-attached devices with system. This is a significant feature because the data contained in RAM will be erased if you turn off the system. It is crucial to record that evidence while such system is still running. The Helix tools also has an enterprise edition that can run live over the network to protect and catalog the evidence found. This tool can also monitor the employee usage, and can also capture the screenshots of several computer screens. This multi-tasking side of the Helix to be considered as of great significance for some investigators but also can become deleterious for others.[410]

9.2.3. ILook:

The ILook was formed by Elliot Spencer, and was statutorily got funded through the government until 2008. The latest version of the tool was 8.0.18 version. ILook is a comprehensive suite of computer-forensic tools mainly used for acquiring and to carefully analyze almost all the digital media. It is compatible with and can support a huge variety of file systems. It is not provided with free trial or it is also not open source, but rather it is more a commercial kit. ILook has built-in file salvage mode in order to get back and recover the removed or deleted files.[411]

9.2.4. EnCase:

While all the above mentioned tools are the legitimate tools, EnCase may be considered as the most widely applied and recognized law-enforcement utility tool towards computer related forensics. The present and latest version now which is in use is EnCase

[410] e-fense :: Cyber Security & Computer Forensics Software, , http://www.e-fense.com/products.php (last visited Jul 28, 2020).

[411] ILook Investigator, , http://www.ilook-forensics.org/ (last visited Jul 28, 2020).

almost everywhere. The extensive and effective training in this product follows with the version of EnCase. This tool actually contains multiple distinct products for various purposes. EnCase most suitably operates under a Windows environment.[412]

9.3. PROCURING EVIDENCE FROM OPERATING SYSTEM:

Any application can be used to communicate over the Internet can significantly contain evidence. The web browsers surfing, official e-mails, and chat conversations are some common for evidence.

Based on the computer related crime in question, one might search evidence from the browser. Generally, in the cases of child pornography, the web browser may contain direct evidence of the specific crime. Although, in almost every computer related crime case, it may provide indirect evidence. For instance, if a person is suspected of having breached a password to perpetrate into a server and hack the financial data, there may be some trace of indirect evidence in such person's browser. It may find the person had recently searched for techniques of breaching the passwords and they may have downloaded certain password-breaking utilities.[413]

Although, the information that might not be just incriminating can be beneficial in understanding the crime. While surfing the Internet Explorer, using the toolbar and referring the complete browsing history for such user. The address bar covers only those web addresses which is typed in and they might be remained without removing. Another thing which several people forget to clear is their forms. Many browsers save the search items that had been previously searched or entered.

Chat conversation is the most frequently used tool for communication. Any planning relating to the criminal act could be discussed through the private chat-room discussions. Trafficking relating to the stolen products, prostitution, and various non-computer crimes mainly require the communication between concerned parties. Chat

[412] EnCase Forensic Software - Top Digital Forensics & Investigations Solution, , https://www.guidancesoftware.com/encase-forensic (last visited Jul 28, 2020).
[413] katharina.kiener-manu, *Cybercrime Module 6 Key Issues: Handling of Digital Evidence*, //www.unodc.org (last visited Jul 28, 2020).

rooms becomes the significant way for such criminals to communicate and same may be used for purpose of the investigation.

The Operating System contains the logs that may provide a significant wealth of information. Such System logs many times reflects login attempts, such as, failed or successful, as well as several alerts which the operating system has given. Several Windows Server versions also contains every reboot of such system in their logs.

Many times, people just delete the files they feel which may become incriminating. Whether such files contain spyware, child pornography or any other dangerous documents, the criminal may remove such files. Although, for the investigator, it may be possible to recover such files back. Files are saved under certain drive, and the operating system keeps a track containing all such files on the system's hard drives. Mainly based on the operating system which the computer is running, there may be possible to find ways to retrieve such removed files.

Moreover, there are several other sources for evidence such as Tracing the IP address, collecting the E-mail Evidence, procuring network evidence from Routers, collecting evidence through a Cell Phone, collecting the evidence through system Firewalls, containing the evidence through Intrusion Detection Systems (IDS), etc.[414]

9.3.1. Slueth:

The Sleuth Kit is a comprehensive command-line based tools that are accessible openly as a free download. They all can be made accessible through the http://www.sleuthkit.org/sleuthkit. Such tool-set may not as rich or easy in use as the EnCase, but it can be an optimum option towards the budget conscious organizations. The common among the utilities included is ffind.exe. It contains numerous options. There are options to find for a given file or to trace only the deleted parts of a file. This specific utility is optimally used when aware about the certain file searched for; although, it may not be a good option for a general search.

[414] *Ibid.*

There are a various utilities installed in the Sleuth Kit, but several users may find using the command-line utilities to be tedious. Although, a GUI which has been formed for the Sleuth Kit is called as the Autopsy and it is made accessible at http://www.sleuthkit.org/autopsy/download.php.[415]

9.3.2. The Dcalifrniaisk Investigator:

Disk Investigator is provided as a free utility which introduced as a graphic user interface (GUI) for the users of Windows. It can be installed from the website http://www.theabsolute.net/sware/dskinv.html. It is not a premium complete pro level product such as EnCase, but it is significantly easy to use. When the utility is first launched, it will present a cluster wise view of the hard drive in the hexadecimal lingual format. Through the 'View' menu, check on directories or the root. The Tools menu provides for the search of a certain file or to recover any removed files.[416]

9.3.3. The Computer Online Forensic Evidence Extractor:

This software tool (also called as, COFEE) was formed by Microsoft specially for the use by law enforcement departments. It is an online based tool which is being provided without any cost to the law-enforcement agencies by Microsoft. This tool is meant to be very easy to use so that with optimal training, any law-enforcement agent can tackle the tool. It is also meant to be worked on live based systems. This tool has the capabilities to operate the following tasks:

a) Decrypting the Password.
b) Search a computer's Internet activity.
c) Analyze what is live in the sensitive memory.

COFEE was initiated and developed by a senior investigator of the Microsoft's Team of Internet Safety Enforcement, Anthony Fung. Mr. Anthony Fung is a former law-enforcement officer of the states and possess the professional knowledge regarding the needs of law-enforcement officers. Further, additional details can be known about the COFEE at http://www.microsoft.com/industry/government/solutions/cofee/. This machine

[415] The Sleuth Kit, , https://www.sleuthkit.org/sleuthkit/ (last visited Jul 28, 2020).
[416] Disk Investigator, https://www.theabsolute.net/sware/dskinv.html (last visited Jul 28, 2020).

is mainly an easy-to-use wrapper among the several other before-existing forensic utilities. It is also to be highlighted that the hacker's community has already formulated a strong response against the COFEE. The tool such as DECAF is a machine mainly formed to do the obstruction of COFEE. DECAF is an acronym commonly used for the Detect and Eliminate Computer Assisted Forensics. It avails the real-time monitoring towards COFEE signatures and regularly attempts to interfere and intervene the running operations of COFEE. For instance, if COFEE is detected the device running on a USB device, then DECAF will eject that device.[417]

9.4. COLLECTION OF DATA:

Information through the survey was collected and analyzed using Google Form & its Statistics. The intention is to mainly investigate if they had experienced or became victims of cybercrime and if so, where they reported the incidents and the final actions. The instruments used during the study included a web-based survey, telephonic interviews, recorded statements, face-to-face interviews, case experiences and the questionnaire.

Moreover, data collected was analyzed after pilot testing to check whether such organization faced any sort of technological crises while professional operations and the response of employees towards such issue mainly with the view of cyber related crimes and also to get pragmatic opinion over the present penalties provided under the IT Act, 2000.[418]

9.4.1. Questionnaire:

After Pilot Testing, a set of questionnaire was distributed to the sample population. The questionnaire survey queried incidents like E-mail bombing, Data diddling, Salami attacks, Virus/worms attacks, Logic bombs, Trojan attacks, Internet Time Thefts, Web Jacking, Obscene mails faced by the technology based organizations in India who all participated. Among the questionnaire that were distributed, most professionals responded

[417] Michele M. Jordan, *Computer Online Forensic Evidence Extractor (COFEE)*, SECURITYWIZARDRY.COM , https://www.securitywizardry.com/products/forensic-solutions/forensic-toolkits/computer-online-forensic-evidence-extractor-cofee (last visited Jul 28, 2020).

[418] Information Technology Act 2000 | Ministry of Electronics and Information Technology, Government of India, *Supra* note 253.

positively and were analyzed accordingly. The participants consisted of students, researchers, the business community, community workers, law enforcement officers and lecturers.

9.4.2. Interviews:

Interviews with senior professionals of organization were conducted to shed more light upon the non-existent cybercrime records buried inside the knowledge of experienced professionals. The interviews were conducted with many officers as well as the sample population to get the pragmatic responses upon the adequacy of present laws relating to cybercrimes in India.

9.4.3. Web Based Survey:

E-mail and Social Media Communications were made to record the information and to find the relevant population in recording the responses and also time saving mode for the sample population and also for general people to respond the provided questionnaire.

9.5. Statistical Analysis:

Google open access tools[419] and IBM's SPSS tools[420] are used while creating statistical analysis of the conducted survey. SPSS provides cumulative percentage through ratio analysis of selected options by the respondents. Google tools provides a comprehensive and flexible statistical and data structure analysis. Google helps to create forms, sheets, charts and tabulated reports relating to distributions and trends and conduct descriptive statistics. Google tools are openly available platform and can be comfortably used by almost every organization by telecommunication, banking, finance, higher education and market research.

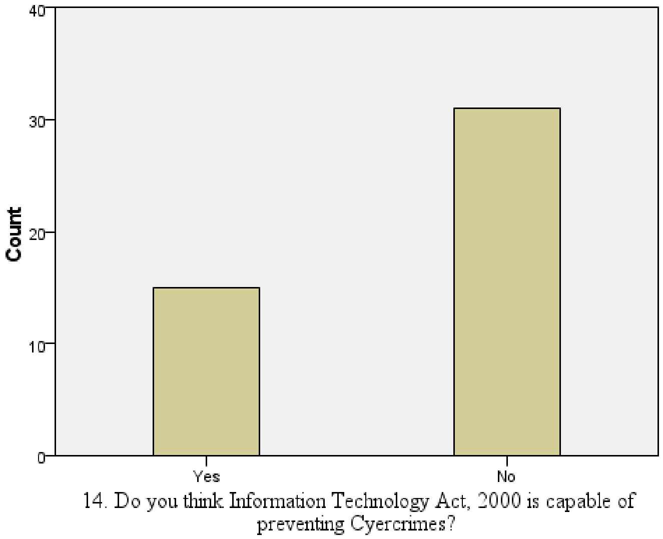
Based on the responses collected from Forty-Six respondents, the data was analyzed through phases from various bar graphs, circular pie charts and tabular charts to

[419] Google Open Source, OPENSOURCE.GOOGLE , https://opensource.google/ (last visited Jul 29, 2020).

[420] SPSS Software - India | IBM, , https://www.ibm.com/in-en/analytics/spss-statistics-software (last visited Jul 29, 2020).

record the respective responses separately and to find out the mean percent of options selected by the respondents, mentioned as.

9.5.1. Bar Graph with Table analyzing the position of Information Technology Act, 2000.

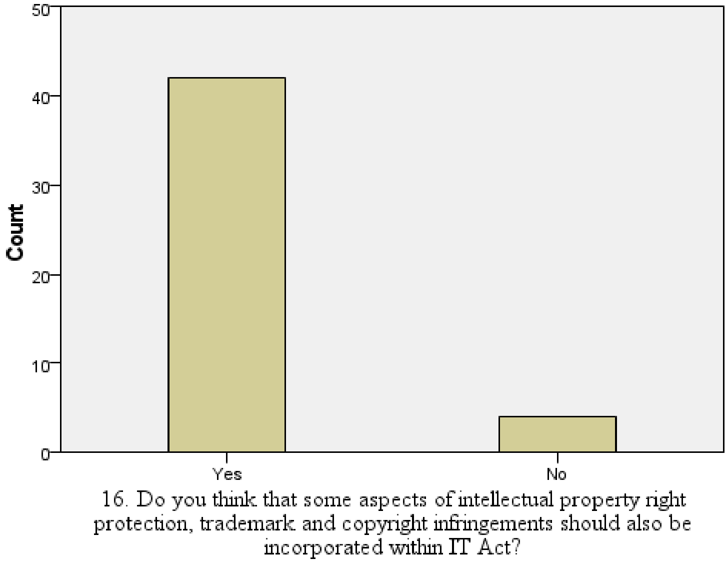


Options	Respondents	Positive Percent	Cumulative Percent
No	31	67.4	67.4
Yes	15	32.6	32.6
Total	46	100.0	100.0

The above mentioned data taken from the professionals working in IT related Indian Organizations clearly shows that, it is important to enhance the provisions of Information Technology Act, 2000 along with rapidly changing technologies, requirements and times to bring domestic organizations at par with IT related global leading bodies and to make country more secure while indulging in any new technologies.

The subsequent pertinent issue addressed is relating to Intellectual Property Rights that, some aspects of Intellectual Property Right Protection, such as trademark and copyright infringement to be incorporated under the Information Technology Act, 2000, mentioned as.

9.5.2. Bar Graph with Table analyzing the inclusion of IPR related protection under Information Technology Act, 2000.

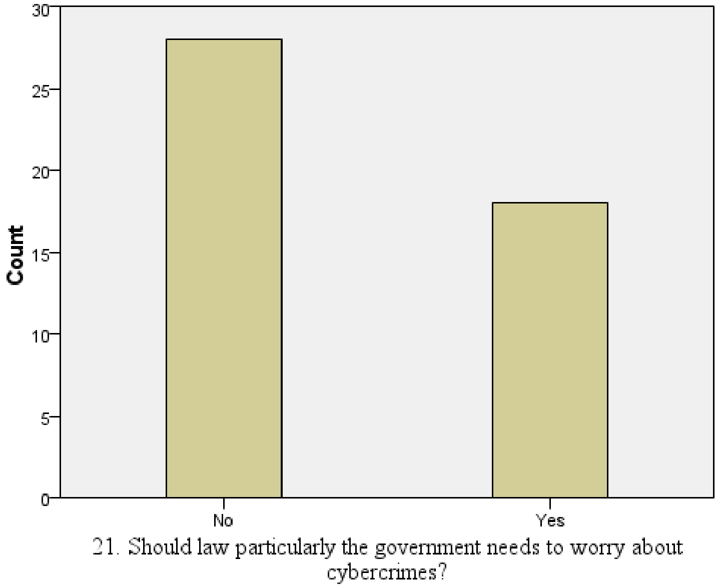


Options	Respondents	Positive Percent	Cumulative Percent
No	4	8.7	8.7
Yes	42	91.3	91.3
Total	46	100.0	100.0

The mentioned statistics clearly shows that major responses demand for the additional IP related remedies and protections to be included under the Information Technology Act, 2000 to provide extra protection to Intellectual Property owners related to any technology or technological based works.

For any sort of crises in the country, is it only government who should be blamed or the citizens also have some responsibilities towards it. Another area upon which it is crucial to shed some light deals with the responsibilities relating to the growing cases of cybercrimes in India, especially, the cases faced by Indian Organizations nowadays, should law alone particularly government worry about cybercrimes, the analyzed data of responses shows that.

9.5.3. Bar Graph with table analyzing the responsibilities towards cybercrimes.

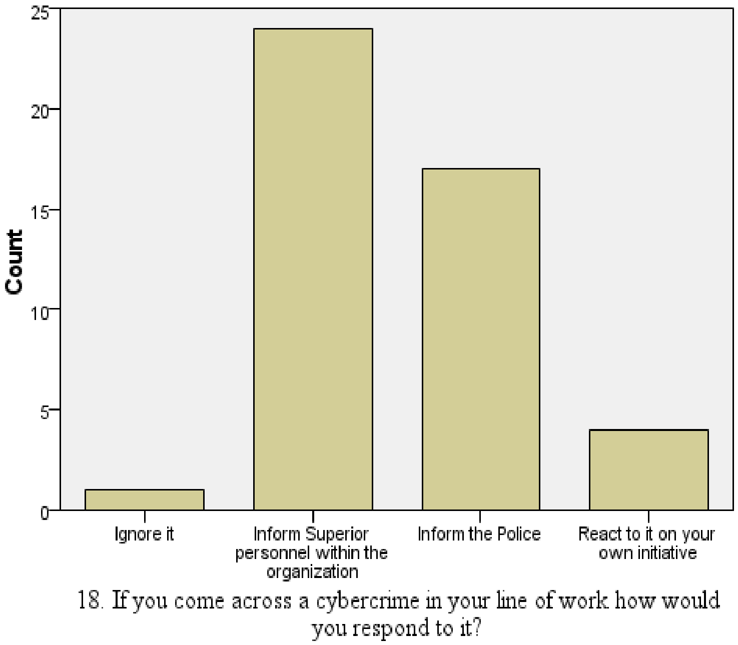


Options	Frequency	Percent	Valid Percent	Cumulative Percent
No	28	60.9	60.9	60.9
Yes	18	39.1	39.1	39.1
Total	46	100.0	100.0	100.0

The above mentioned contention analyzed through such collected data indicates that solely government or legal authority is not to be held responsible while tackling cybercrimes, but also people to be held responsible for their actions who all are operating or facing such issue or handling it. The technology usage system bears some responsibilities on the users as well to secure their personal data efficiently and to become more responsible for their own actions.

After dealing with legal enforcement related issues of cybercrimes faced by organizations in India, it is important to also address the experiences of Indian organizations and their working employees' while dealing with cybercrimes related problem. Whether they came across any cybercrime in their line of work how would they respond to it. The sample was collected from different areas of employment; the responses are as.

9.5.4. Bar Graph with Table analyzing responses to Organizational Cybercrimes.



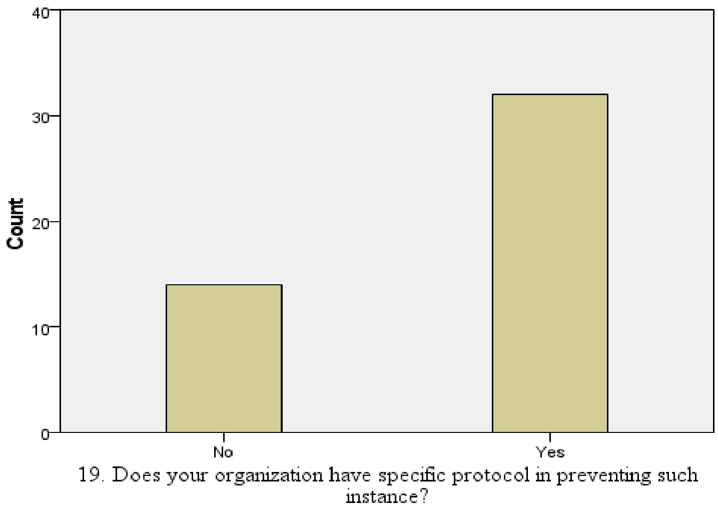
Options	Frequency	Percent	Valid Percent	Cumulative Percent
Ignore it	1	2.2	2.2	2.2
Inform Superior personnel within the organization	24	52.2	52.2	54.3
Inform the Police	17	37.0	37.0	91.3

React to it on your own initiative	4	8.7	8.7	8.7
Total	46	100.0	100.0	100.0

The above mentioned responses clearly shows that major portion of data supports the chain of command and to inform their superior. Through interviews it was revealed that such responses are due to less awareness among the employees about the available options to deal with such problems, so they report it to their superior. But, this step may also lead to suppressing of problems than curbing it. Sometimes, superiors may suppress such problems to maintain public image of their organization which may become deadly in long run. Thus, it is important to make working professionals aware about available options for reporting cybercrimes cases directly to the concerned legal authorities.

Given that, the connected issue is also raised, that is, whether their organization have a specific protocol to prevent such instances, the responses are as.

9.5.5. Bar Graph with Table analyzing the use of protocol to prevent cybercrimes



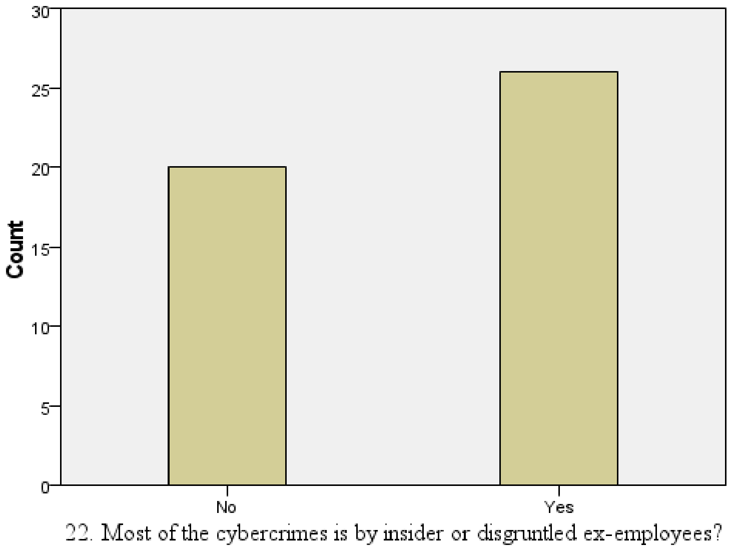
Options Frequency	Percent	Valid Percent	Cumulative Percent

No	14	30.4	30.4	30.4
Yes	32	69.6	69.6	69.6
Total	46	100.0	100.0	100.0

From the above mentioned analysis, it is apparent that many Organizations in India have specific protocol to prevent cybercrimes still the cases of cybercrimes are growing with great pace. So, it is important for the technology based organizations to apply best suited crises management model to enhance protocol system as well as to curb the problems of cybercrimes more effectively.

Another contention which is raised to scrutinize the internal management of Indian organizations while facing cyber-attacks, that is, whether most of the cybercrimes are done by insiders or disgruntled ex-employee, the analyzed data shows that.

9.5.6. Bar Graph with Table analyzing the role of internal management of Organizations towards cybercrimes.



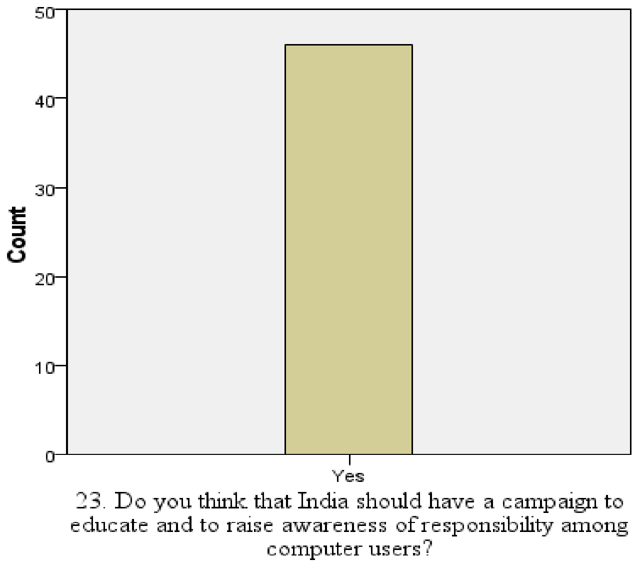
			Valid	Cumulative
Options	Frequency	Percent	Percent	Percent
No	20	43.5	43.5	43.5

Yes	26	56.5	56.5	56.5
Total	46	100.0	100.0	100.0

The graphical representation and tabular analysis shows that, the ratio of cybercrimes done by insiders or disgruntled ex-employees is relatively high which indicates that Indian organization still faces weaker internal management and needs to develop stronger internal management policies and teams to effectively deal with the cases of cybercrimes in the organization.

The most important issue addressed while collecting the samples is relating to computer and cyber related education. Whether India should have a campaign to educate and to raise awareness of responsibility among computer users, it was responded as.

9.5.7. Bar Graph with Table analyzing importance of computer related education in India.



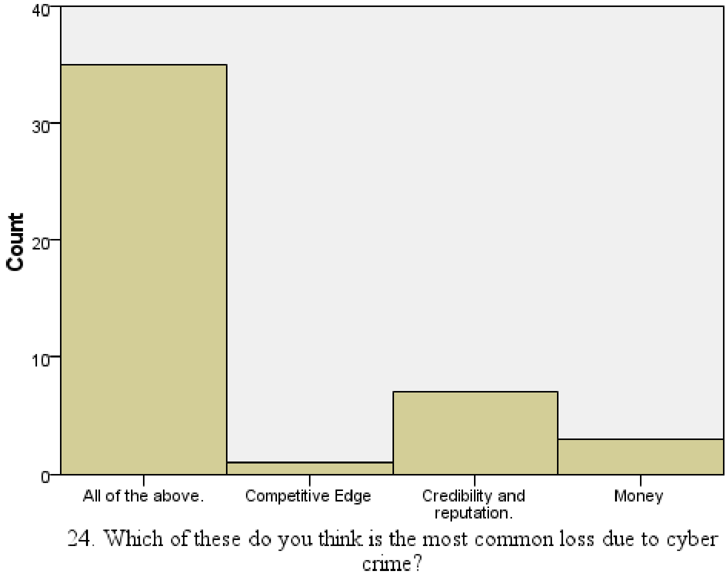
Options	Frequency	Percent	Valid Percent	Cumulative Percent
No	0	0.0	0.0	0.0
Yes	46	100.0	100.0	100.0

Total	46	100.0	100.0	100.0

The provided data analysis clearly indicates that, India needs a campaign to educate and to raise the awareness for the responsibility among the computer users, ultimately, also educate the employees which results in required awareness and such initiative may help organizations in enhancing their work productivity.

Another problem highlighted relating to the most common losses faced by organizations or working professionals due to cybercrimes raised to understand is there any common target areas behind such crimes committed by the perpetrators. The responses are as.

9.5.8. Bar Graph with Table analyzing the common losses to organizations due to cybercrimes.



Options	Frequency	Percent	Valid Percent	Cumulative Percent
All of the above.	35	76.1	76.1	76.1

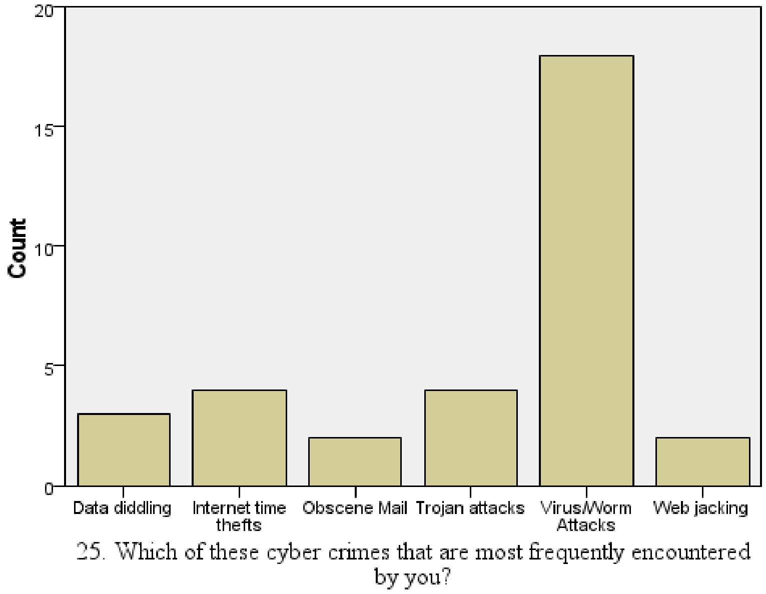
Competitive Edge	1	2.2	2.2	78.3
Credibility and reputation.	7	15.2	15.2	93.5
Money	3	6.5	6.5	6.5
Total	46	100.0	100.0	100.0

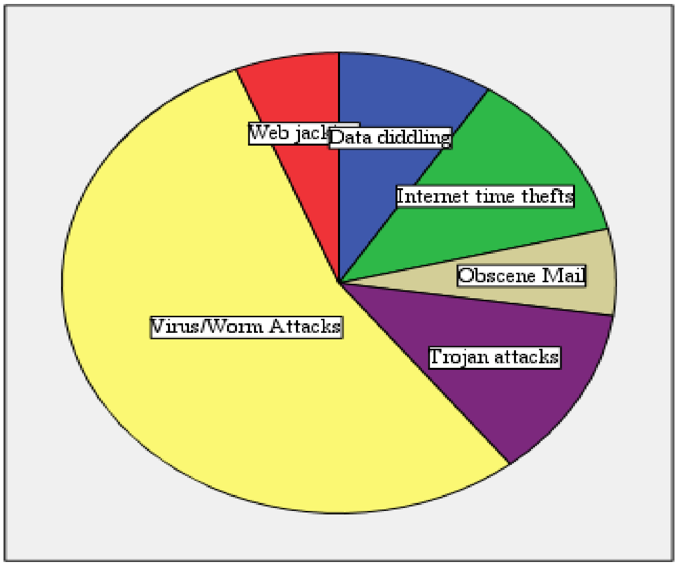
The above mentioned analyzed data indicates that there is no specific reason shown for which cybercrimes are committed by such perpetrators but their action creates general disaster for the organization as a whole, so, it is important for organizations to take cybercrimes seriously and to prepare themselves beforehand.

The incidents of cybercrime may not only cost money or competitive edge but also harms its creditability and reputation among people in their market area or may even result into their permanent close down.

The final but most important contention addressed relating to the experiences of Indian organizations or their working professionals while dealing with cybercrimes related problem. They were asked which cybercrimes that are encountered by them during their work. The responses and data collected from the organizations of India is analyzed as.

9.5.9. Bar Graph, Pie Chart with Table analyzing the cybercrimes encountered by Indian Organizations.





Cyber Crimes	Frequency	Percent	Valid Percent	Cumulative Percent
Data diddling	3	6.5	6.5	6.5
E-mail bombing	13	28.3	28.3	34.8
Internet Time Thefts	4	8.7	8.7	43.5
Obscene Mail	2	4.3	4.3	47.8

Trojan attacks	4	8.7	8.7	56.5
Virus/Worm Attacks	18	39.1	39.1	95.7
Web jacking	2	4.3	4.3	100.0
Total	46	100.0	100.0	100.0

The above mentioned analysis indicate that the majority of technology based organizations in India are prone with the problem of Virus/Work attacks followed by e-mail bombing which shows that it is crucial to create professional protection systems and precautionary measures to avoid such attacks while dealing with work related data in office or even if working remotely from office.

The statistical analysis was conducted to analyze two phases of technology crisis, to scrutinize the proper enforcement of Indian cyber laws by organizations and another is to analyze the experiences of Indian organizations related to cybercrimes and actions taken by them to prevent related problems. By correlating the analysis comprehensively, it is to be suggested that through campaigns to educate and make working professionals aware about their responsibility to protect their organization from cyber related problems as the cases are growing rapidly.

Moreover, it is important for the Indian organizations to adopt suitable crisis management model to tackle these unexpected problems in advance and it is also important to frequently update the current cyber laws to meet the pace of changing times, technologies and face of crimes in India.

CHAPTER 10

SUMMARY, CONCLUSION AND SUGGESTIONS

"It is in the whole process of meeting and solving problems that life has its meaning ... Wise people learn not to dread but actually to welcome problems"

- M. Scott Peck
The Road Less Travelled

10.1. FINAL OVERVIEW:

Crisis is one of the most faced problem by the Organizations in India recently. Crisis Management becoming a new corporate discipline is gaining greater importance all across the world. Although there is no much studies conducted in India in this regard but certain similar portions can be referred from the foreign countries as well. Creating technological management awareness on this concept with regards to India and guiding the organizations in by showing them greater importance towards the crisis planning and crisis communication which have eventually become the need of the day in recent times. With this work, it has also been attempted to find out the extent to which independent factors like Age, Education, Experience and Position and the organizational variables like nature of organization and Line of Activity have influence on Crisis Awareness, Crisis Requirement, Crisis Planning and Crisis Communication.

It is rightly quoted by Mr. Waleter B Wriston that, "the technology has made us a 'global community' in the literal sense of the term. Mankind now has a completely integrated information marketplace capable of moving ideas to any place on this planet in minutes. Information and ideas will go where they are wanted and stay where they are well treated. It will flee from manipulation or onerous regulation of its value or use, and no government can restrain it for long".[421]

A questionnaire was designed with the formal consultation with eminent professors and executives of reputed organizations. For the reliability, the questionnaire was also pre-

[421] Douglas Martin, *Walter B. Wriston, Banking Innovator as Chairman of Citicorp, Dies at 85*, THE NEW YORK TIMES, January 21, 2005, https://www.nytimes.com/2005/01/21/obituaries/walter-b-wriston-banking-innovator-as-chairman-of-citicorp-dies.html (last visited Jul 29, 2020).

tested through a pilot study. Through the suggestions given by the respondents the final structure of the questionnaire was improved. A nation wise survey of cyber law indicates that only a few countries have updated their cyber law to counter the cyberspace crime effectively, while many of them have not even initiated steps to frame laws for policing against these crimes. This divergent approach of world nations towards the desirability of cyber law poses a real problem in handling the internet crime and at the same time provides ample scope for the cyber criminals to escape detection and punishment. All the nations should therefore, realize the need and urgency for generating awareness about the dangerous nature of cybercrimes which are perpetuating illegal online activities in cyberspace. Cyber criminality is perhaps the deadliest epidemic spread over the world in the new millennium which has to be curbed by adopting a global preventive strategy.

As India is concerned, it has introduced Information Technology Act and amending the Principal Information Technology Act, 2000 through I.T. (Amendment) Act, 2008[422], w.e.f, 5th February, 2009. The amending Act has inserted as many as 15 new cyberspace offences which are punishable under the I.T. Act. That apart, many of the provisions of the Indian Penal Code have been amended to include within it certain criminal acts relating to cyberspace and electronic media.

The speedy development of technology has brought about significant changes in the modern society. But human experience has shown that every technological change bought with it some unpredictable problems, taking advantage of which the perpetrators and law breakers explore new techniques to perpetrate their aimed targets. In fact, technology generated crisis not only affect individuals or a country, but have a widespread ramification throughout the world. Internet is one of that gray zone, that has given rise to the menace of cybercrimes. The computer based global communication system has braked the barriers of the territorial borders, therefore, formulation of a distinct field for online criminal activity warranting global attention.

[422] The Information Technology (Amendment) Act, 2008 – The Internet Democracy Project, , https://internetdemocracy.in/laws/the-information-technology-amendment-act-2008/ (last visited Jul 29, 2020).

Cybercrimes have emanated from the expansion of computer networks. Internet in the current millennium has become omnipresent and also pervasive. It has also brought with it hitherto new issues still unknown to humanity. Internet can also be considered as analogous to the 'high seas' which no one owns yet people of all the nationalities use it. The term 'cybercrime' encompasses within it a unique form of criminal activities conducted in the cyberspace through the mode of global communication technique and information through the internet. It is an inevitable evil having its origin in the more and more dependence of mankind on computers in modern life, the reason being that the computers despite being high technology devices are extremely vulnerable. Thus, whenever any crime or criminal activity takes place with the use of computer, it constitutes a cybercrime. It is because of this sense that 'cybercrime' has been enumerated as 'an unlawful activity wherein the computer is either a tool or a target or both'.[423]

It does not require any special mentioning that Science & Technology has enlarged its ambit by breaking the national frontiers whereas law is still find difficulties in defining and redefining the boundaries for controlling the cybercrimes. With the same course of pattern, the Indian cyber law, particularly, Information Technology Act, 2000, is focused in controlling and prevention of cybercrimes with the territorial jurisdiction of country but missing the fact that it needs inclusion of global cyber criminality provisions for certain segments as well.

Therefore, cybercrimes are such dangerous activities in the cyberspace which may cause damage to a person, property or even to the state as a whole. Being significantly different from the conventional crimes, the law enforcement bodies find it difficult to tackle.

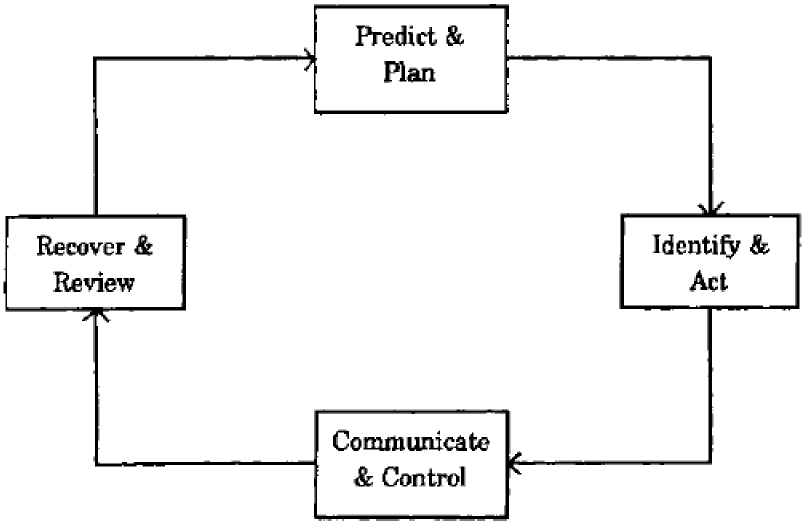
10.2. CONCLUSION:

The overall analysis of the research mainly emphasizes that every technology based Indian organization has to give due importance to the concept of 'Crisis Management'. Planning for technological crisis, Campaign for technology crisis management awareness

[423] Cyber Crimes "an unlawful act where in the computer is either a tool or a target or both" - Strategy - India, , https://www.mondaq.com/india/technology/28603/cyber-crimes-an-unlawful-act-where-in-the-computer-is-either-a-tool-or-a-target-or-both (last visited Jul 29, 2020).

and real time crisis communication are the essential elements which is to be followed by such organizations to maintain stability and growth. In spite of this, if organization faces virtual crisis then they should always have a positive approach to convert a crisis into opportunity. Surviving from crisis provides great opportunity in front of the organizations to reanalyze and reorganize itself to commit it never find itself in such similar situation again. Finding, examining and harvesting the significant success through mutual efforts is the essence behind crisis management.

Figure 10.2.1.: Crisis Management Model[424]



In the context of electronic evidence, it is significant to note that despite the fact that digital signatures have facilitated e-commerce by reducing paper-work and ensuring quick transactions, it has not been widely accepted in India because of the technicalities involved in it and therefore, people in general still believe that paper-based documents are more dependable and trustworthy than the paperless electronic records. The reason being

[424] Crisis Management Model, , https://www.managementstudyguide.com/crisis-management-model.htm (last visited Jul 29, 2020).

that former are tangible and serve as best piece of evidence before a law court. However, with the expansion of e-commerce and legal recognition of e-contracts in business transactions, there is change in the mindset of the people and they are gradually adapting themselves to the new e-environment and finally switching over to paperless electronic transactions.

Cybercrime being worldwide in character, it can adversely affect the person nowhere near from the place or jurisdiction of offence, may it be in the same country or any other country. Therefore, it needs concrete policing at the international level and also requires the serious understanding and participation from the international community.

The jurisdictional problems interrupting the efficient handling of cybercrime investigation results into the widespread inter-connectivity of the computer networks and the supporting infrastructure such as telecommunication information dissemination on the website etc. Although, jurisdiction is a broad concept which refers to whether a court has power to adjudicate, i.e., whether it has personal jurisdiction to try the case and territorial jurisdiction over the location or place where the crime is committed or the parties concerned reside. In case of cross-country cyber dispute or crime, the problem often arises as to the law of which country would be applicable to the case in hand.

10.3. SUGGESTIONS:

Due to the growing dimensions of computer related crimes, it is necessary to adopt the required regulatory legal measures and to enhance the pace of the legal enforcement mechanism to control the problem of cybercrimes with the stern hands. A slight delay in investigation may allow cyber-criminal to erase all the potential data which is prime evidence to evade detection threat, which may cause huge losses to the victim. The grim nature of the cybercrimes is such that the offender as well as the victims does not need to come face to face for executing the crime, which immensely benefits the criminals to continue their criminal activities with same confidence without any fear of being prosecuted or even apprehended. It is because of that a multi-dimensional approach and strong efforts of all the law enforcement functionaries is much more required for proper tackling of cybercrime cases in India. A common cybercrime law which is to be universally acceptable to all the nations may perhaps give a reasonable solution to control the cyber criminality.

The process of crime control mainly requires support and cooperation of institutions, citizens, organizations and the government together. So, a logical strategy to control or prevent the cybercrimes requires active community participation for combating this menace. This requires an active participation of all those who believes that the increasing cases of the cybercrime is a significant threat to the society. It also requires for secure initiatives by the people who are vulnerable to cyber related crimes. They must have adequate knowledge and awareness about the scope, nature and gravity of these crimes and the problems fraught by them. It is noteworthy that media has an essential role to play in informing people against the possible dangers and evil sides of cybercrimes over victims and also for the country and the protective measures which all are important to tackle this problem. It may support in controlling the cases of cybercrimes provided effective implementation of laws by enforcement agencies.

There are other important suggestions to reduce and curb the cases of cybercrimes at national level are as follows:

1. **Net Security be increased:**

Computer based technology has proved to be a beneficial for the society, especially to the commercial world. Most of the commercial, organizational and business transactions are mostly done through internet services at the national as well as the international level. The growing use of computers and internet in the field of trade and commerce has at the same time provided new opportunities for the perpetration of cybercrimes to the offenders for their personal monetary advantages. With the introduction of liberalization and globalization of economy, the organizations now believe that there is a huge and profitable market for commercially exploiting the networks. With the growing dependence on computer in the commercial sector, most of the money transactions are being carried out with the help of computer network making it possible for the cyber criminals to illegally intercept and commit financial frauds. Therefore, it is essential that the reasonable protective mechanism be formed for safeguarding e-banking and e-commerce against apprehended online thefts, frauds or the documental forgeries etc.

With regards to the legality of commercial transactions conducted on the internet, the Securities Exchange Board of India (SEBI)[425] has provided that the trading of securities over the internet will be valid in India which provides legal validity and prevent security frauds and stock manipulations over the internet. An appropriate provision for security of the confidentiality for the online trading, thus, it is also to be incorporated under the Information Technology Act, 2000.

2. **Use of end-to-end encryption system:**

It should be compulsory for all the Indian organizations such as, governmental, semi-governmental as well as non-governmental which tend to the enlarging computerization for the transfer of information and conducting the business transactions, to appoint professional Information Security Officers who should take charge and responsibility for overall security relating to computer resources and they may also be made responsible for any problem or lapse in the computer related security.

The application of the technology relating to encryption may also tend to protect the data and transactions from unlawful and unauthorized access, disclosure or any changes. It also helps to control the crime by providing security to the valuable secret information over inter-connected systems and networks. The law enforcement authorities may develop and provide the use of protected and recoverable encryption services for securing and business data from being manipulated or stolen by miscreants.

Resembling to encryption, there is another technique named as 'steganography', which is used as a protecting shield against network invasion. It is a method for obscuring potential information in a way so as to prevent its detection. It mainly includes language that is not readily discernible to the casual observer.

Moreover, Firewall device is another tool which can be carefully used to provide regular warnings against any attempted attacks or intrusions in the database. It is a complete software application which is designed to monitor data transmission through one computer

[425] Securities and Exchange Board of India, , https://www.sebi.gov.in/ (last visited Jul 29, 2020).

to another over the active network. It can also be used to monitor and control the scale of data transferred over one's computer network.

3. **Intrusion Control:**

A new restrictive method known as the 'intrusion control' may be used for detection, testing and thorough investigation of cybercrime. It is a process which mainly aims for preventing intrusions in the active computer system by facilitating ensured e-security control mechanism. The computer or internet users and e-commerce organizations should verify that technical areas of vulnerability of the related system are kept appropriately controlled so, as data is concerned, following is absolutely protected-

i. Identification and authenticity;
ii. Accessibility;
iii. Accountability;
iv. Accuracy; and
v. Reliability;

Various cybercrime investigations and cases results in that the victim's computer system has been destroyed due to cybercrime attack but the attack source could not get traced or found. So, one of the most essential feature of intrusion control is to trace the security issues so as to provide the computer system fully protected and secured.

The security measures provided under the intrusion control system also includes security against viruses by adopting strategies relating to anti-virus, firewall use, authentication and encryption program.

4. **False registered E-mail ID to be made punishable:**

Cyber perpetrators provide false information while officially registering for an e-mail address for a website as the e-mail service providers does not allow two different addresses to the same person. This misleading information provided over the internet facilitates the criminal to hide his original identity and misguide the investigating authorities in tracing the real culprit. This lacuna has been taken care of by inserting a new

Section 66A in the principal Act by the I.T. (Amendment) Act, 2008[426] which provides that any false e-mail identity registration with a website will be an offence.

5. **Self-regulation by Internet Users:**

Self-regulation is to be implied as one of the reasonable solution to suppress the cases of cybercrime. It is a process of creating a sound code of conduct by accepting a restraint policy by both, the service providers as well as the computer users. Internet Service Providers (ISP) can play a significant role in reducing the cases of online crimes taking certain self-regulatory initiatives. In order to begin, ISPs may collectively create and provide an integral code which is to adhered by them while providing any internet services towards the clients. Also, they may provide the suitable conditions by way of a mutual agreement binding upon the users which restricts them from conducting any illegal activities. Moreover, they can mention under the contract that breaking of any of such conditions would results into the termination of provided internet services.

6. **Reasonable search & seizure regulations:**

The legal enforcement authorities require intensified approach while dealing with any form of cyber criminality. Especially, the present legal regimes should allow such legal enforcement bodies to complete their tasks without any fear or any external pressure. Such agencies should be provided certain rights to collect relevant details from the concerned service providers as may be required to conduct internet crime investigation, however, without violating or breaching any basic fundamental and privacy rights of the parties. The search and seizure provisions relating to cybercrimes requires liberalized approach so as to provide the investigating authorities or the police to apprehend cyber criminals in time and initiate appropriate proceedings against such criminals.

7. **Increase in usage of Voice Recognizer and Filter Software:**

The technology is the ultimate tool whose loopholes created the problem of cybercrimes. So, firstly, to prevent its misuse, the areas where the usage of computer is

[426] Section 66A of Information Technology Act: Punishment for sending offensive messages, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-66a-punishment-for-sending-offensive-messages-through-communication-service-etc/ (last visited Jul 29, 2020).

required as a means for the purpose to carry on regular life activities to be made equipped with certain protective and safety devices to provide security against the unauthorized access to the computer. For instance, the new voice recognition system which depends on voice pattern to get unlocked to be effectively used, while organization may set it up for high level professionals. Moreover, anomaly detection software, traces the unusual or hostile pattern relating to computer use, aids the computer users or organizations to prevent and frustrate the perpetrators. Also, filter software mainly provides protection against the known or possible threats.

8. **Requirement of Strong Cyber Forensics and Biometric technology:**

To facilitate the appropriate technical assistance to the investigating authorities for the purpose of identification, tracing, preserving and extracting the digital information from host computer to provide it in the form of evidence for cybercrime in front of the Hon'ble Court of Law. The modern cyber forensics technique mainly includes three elements, such as, internet forensics, computer forensics and software forensics. The inter-relativity of all three elements provides a comprehensive cybercrime detection mechanism in the modern times.

i. **Cyber forensics**: It is also named as 'network forensics', it mainly deals with digital evidence that is provided across the large computer network. The main intention of cyber forensics is to extract the evidence and trace the intent and identity of the cyber criminals and also to determine the consequences of such crime on the victim and society.

ii. **Computer forensics**: it deals with the chain of evidences seized from the prime crime scene through the extraction of hidden or removed information from the system disks.

iii. **Software forensics**: it mainly deals with the creator of such dangerous code for perpetration and provides required hints to identify the criminal behind cybercrime.

The biometric technology plays significant role for the identification of real perpetrator behind cyber related crimes. Biometric includes digital analysis of parts provided from a person’s physical characteristics that are different to that person. For instance, the codes developed from critical analysis from fingerprints, retina scans, footprints, body odor etc. may give crucial clues to identify the person guilty for cybercrime, though it required to be corroborated through other relevant evidence.

9. **Need for intensive Research & Development Centre for Cybercrimes:**

One of the important approach to prevent cybercrimes in India is to provide awareness among the computer users or organizations relating to the possible threats emanating from manipulation of information or systems for unlawful gains. In various cases, the internet users remain unaware about they are being online, they may become trapped to cybercrime or may unknowingly involve themselves in an activity which considered as an offence although they never intend to commit it. Specifically, the adolescents who, for the sake of entertainment or enjoyment, switch over to pornographic websites and make themselves become a victim towards cybercrimes. Possibly, this can be eradicated by making aware the internet users about the possible threats and outcomes of such unlawful activities which they unknowingly or ignorantly done over the internet.

At this juncture, it is real important to mention that India requires the establishment of National Digital Crime Resource Centre which may include the people as members from various segments of society, such as, software technical experts, forensics and law experts, hardware experts, member from legal enforcement agency, member from Reserve Bank of India and member from Central Bureau of Investigation, they have role to work collectively to enumerate people about the possible threats of various cybercrimes and their legal regulations among the internet users by setting up the model standard code through the help of government to make cyber world a secure place at national level.

10. **Requirement for International Cyber Law Regulation Mechanism:**

The old conventional laws relating to the disputes of property may not be considered fully valid to protect the unauthorized access and manipulation of potential information through computer networks. So, there is dire requirement for restructuration of the substantive as well as the procedural laws for the computer related crimes through that the frequent offenders may be brought to justice. Currently, the definition of cybercrime differs from country to country based on the cases of such crimes and their sensitivity in that state for them. Due to the lack of any universally accepted definition of cybercrime, approach and inquiry relating to cross-border cybercrime cases are conducted in accordance to the procedural law of the area where such cybercrime is committed.

The question relating to a nation's jurisdiction in case of a cybercrime conducted outside the country but having disastrous outcomes on that country itself, makes it baffling and still remains unresolved as there is no uniform consciousness among different nations over this important issue. The uncertainty of jurisdiction with regards to crimes committed through computers at remote location has made such commission of crime easier, whereas, penalizing the offenders thereof became more difficult. Thus, now the need of an hour is drafting and finalizing a uniform cyber regulations with the common consciousness between all countries of the world.

The nature of cross-border jurisdiction relating to internet and lack of sufficient international cooperation to meet the problem for cross-border cyber criminality aids criminals in escaping arrest and the prosecution. Therefore, to resolve such jurisdictional problems relating to the cybercrimes, it has been exclusively suggested that an International Cyber Tribunal with international jurisdiction to be set up with regulations relating to investigate, trial and punishment for cyber criminals.

11. **Need of Universal code to resolve IPR related disputes:**

The information technology revolution during the closing years of 20th century has opened scope for new variety of disputes in IPR regime, both at national and international level. The resolution of these disputes needs a Global Code of Digital Law to be developed which should have universal acceptance all over the world. This is all the more necessary in view of the expanding dimensions of IPR transactions having multi-national ramifications.

12. **Active role of Interpol and Computer Security Team:**

Presently, the 'INTERPOL', that is, International Police Organization, functions at the international level to provide the police cooperation among different countries and facilitate required tools and needed services for effective trace and investigation relating to the cross-border cybercrimes, however, its efficiency hampered due to the lack of desired co-operation from the affected countries. INTERPOL has broad connection linking to almost 200 countries with the General Secretariat of Interpol and it is mainly involved in crusade against cross-border cyber criminality. Through this mutual connection, the countries communicate through e-mails to send information about cybercrime and criminals to the General Secretariat office which incorporates it in the globally provided database and then provide such data access to every connected country or to those countries who owns such authorized information.

Along with being a INTERPOL member, various countries have created their own Forum of Incident Response & Computer Security Teams (FIRCST) to prevent and treat cybercrime within their domestic territorial borders. However, there is still need for the creation of uniform forum among the members at international level to share the transmission of relevant information relating to cybercrimes and perpetrators and also to exercise preventive measures to deal efficiently with this menace.

13. **Expert Mechanism to deal with Cyber Terrorism:**

The problem of cyber terrorism has totally changes the meaning of traditional concept relating to terrorism as the advent of information technology has facilitated terrorists to exercise more sophisticated and destructive technology and resources to attack their targets. They may not directly target the defence system or government departments but they can directly target the potential working organization of targeted country and its destruction leads to collapse of country’s economy which sends negative message at international level about this problem. Thus, it is highly suggested to deal with this problem by creating and applying e-security technology and adopting stringent penal policy both at the national as well as international level. It may be suggested that India can also appeal to the SAARC forum to have consensus among the member states about the requirement of the joint efforts to control the cybercrime cases, specifically, cyber terrorism through common co-operation. Appropriate actions should also be made to possess advance cyber technology from the developed countries by acquiring a uniform Code of Cyber Legislation.

14. **Expert Cybercrime Investigation Cell for High-tech Cybercrimes:**

A cybercrime Investigation cell was notified in September, 1999 under the Central Bureau of Investigation with effect from 31st March, 2000. It is headed by Superintendent of Police, who possess power to investigate the offence under Chapter XI of the Information Technology Act, 2000, empowered to investigate into high-tech cybercrimes and has jurisdiction all across India.

In consonance to the establishment of Cybercrime Investigation Cell, there are setting up of cybercrimes police stations by the respective state governments. Karnataka was first state to setup Cybercrime police station dated 30th August, 2001. These cells have qualified and trained police officials with assistance of cyber experts whenever required to investigate cybercrime cases. But still there are several states who does not have special police cyber cell. Therefore, it is suggested that every state should have Cybercrime police stations trained and equipped with modern technology and cyber experts staff where cybercrimes complaint can be lodged online so that sensitive cybercrime could be investigated efficiently and effectively. The trained police officials working under this cell to be provided power to conduct search and seize relevant information with the prior permission of magistrate against cybercrimes.

15. **Video conferencing and e-judiciary for speedy justice:**

The National Policy of Information and Communication Technology (NICT)[427] proposed the three phased e-judiciary framework to speedily dispose the cyber related cases. To develop the suitable standards and rights to deal with crimes relating to cyberspace. The National e-court Project initiated in the year July, 2007 for the formulation of e-judiciary as well as e-governance grid including India’s entire judicial system may ensure transparency, fairness and speediness towards the handling of cybercrime cases. It may also eliminate workload of the courts and provides speedy settlement of cases as also eradicate problems relating to the paper based records, such as, their maintenance, extraction, collection and retention etc. it is comparatively easier to compile and retrieve electronic record.

[427] NICT - Toppage | National Institute of Information and Communications Technology, , https://www.nict.go.jp/en/ (last visited Jul 29, 2020).

It does not require any special mentioning that digitalization may enhance the working productivity of judiciary. It may provide easy accessible database supporting judges, lawyers and court working officials as well as to parties.

16. **Quality Cybercrime Reporter or Cyber Law Journal:**

The statistics relating to cyber related crimes sometimes does not reflect the exact position of cases of cybercrimes. Many victims defer to report the cases relating to cybercrimes as they apprehend about unnecessary harassment and may also cost time and money over litigation which may lead to nowhere. Mainly, the organization avoids to report incident due to fear of adverse publicity such as reduction in goodwill, embarrassment or loosing of competitive edge. The lack of adequate technological expertise while handling the cybercrime on behalf of law enforcement agencies may also become a contributing factor for non-reporting of such cases by the victims.

However, as continuous rise in the cybercrime cases and increase in the cases before court for the adjudication, it is pertinent to note and publish quality content to spread awareness by raising a quality of ‘Cyber Law Journal’ or ‘Cyber Crime Reporter’ for not benefitting the judiciary but also to the member of the society.

17. **A step towards right direction- IT (Amendment) Act, 2008:**

In the change of time and advancement in technology, there are several changes bought over this period of time, still the menace of cybercrime is reaching at the alarming state due to continuous change in technology and thus, it is required to take concerted step to formulate a universal mechanism to prevent these crimes. Although, the introduction of amendment in Information Technology Act in 2008 provided reasonable success in providing remedies to computer users by developing the legal reach upon new online criminal activities and also aware people about such crimes through special mentioning of crimes. Although, the Act still suffers certain shortcomings relating to security for web transactions, it does not include provisions against securities frauds, internet stock trading frauds, however, the Securities and Exchange Board of India provided notification relating to online trading of securities as valid and legally recognized.[428]

18. **Digital Time Stamping System (DTS):**

The Information Technology Act, 2000 provides transactions through e-signature to be recognized and made enforceable by law although, there is no particular mechanism or system to know exact location and at what time such electronic document was formed and signed electronically. It creates the non-availability of any reliable evidence to provide the exact date and time when such disputed electronic document prepared and electronically signed leaves enough margin for uncertainty resulting in weakening of the prosecution case in such cybercrimes. This issue may be resolved by introducing an electronic device called as 'Digital Time Stamping System' (DTS)[429] mainly to monitor electronic transactions. It includes an apparatus called as 'Tamper proof Box' under which a highly protected time-stamping server is applied to create Digital Time Stamps (DTS). The system has been a great success in the United States for many years.

19. **Inclusion of Extradition Treaty:**

The present information technology law recognizes the extra-territorial jurisdiction of cyber law but it may be efficiently applied in the cases where perpetrator happens to be from a country with which India does not have extradition treaty. It is suggested that it may be resolved by making a suitable amendment to include cyber criminals from non-extradition countries and in essential circumstances they can be brought and tried in India and to be prosecuted in accordance to the established principles of relevant international law.

20. **Special Cyber Courts in India:**

[428] The Information Technology (Amendment) Act, 2008 – The Internet Democracy Project, *Supra* note 421.

[429] decoding time-stamp (DTS), , ATSC : NEXTGEN TV , https://www.atsc.org/atsc-glossary/decoding-time-stamp-dts/ (last visited Jul 29, 2020).

Due to lack of expertise in dealing with the increasing cybercrime cases in India. It is to suggest the formulation of special cyber courts with trained judicial officers, lawyers and police officers to expeditiously deal with the rising cybercrime cases.

21. **Facility of high speed internet across India:**

Currently, due the crisis of COVID-19 pandemic, more or less, every type of work depends upon the use of computer and internet, while there is still large portion of population find it difficult to understand the usage of computer and related technology systems, pointless to say anything about cybercrimes and it may form a digital divide among the people of country. Therefore, government should provide more access to computers and internet at remote places of India as they already promised for the rural areas to provide Common Service Centres (CSCs) – broadband enabled computer kiosks that offers the range of Government-to-Citizen and Business-to-Customer services, along with the access to the internet.

22. **Quick blocking mechanism of Errand Websites:**

An advanced screening system to be placed at bandwidth landing station to preliminarily block the websites and web blog that are apprehended as potential threat to the national security of India. The launched system to be capable for blocking websites at sub domain stage and protecting ISPs from a sweeping shutdown. It is suggested that government needs to realize that most suitable way to eliminate such site is through URL-based blocking system fixed at the international gateways. After such system is in right surface, the Department of Telecom (DoT) can direct ILD players, who own and manage the landing stations and may block a specific provided URL at the sub domain stage.

For instance, 26/11 crisis of Mumbai Blasts

23. **Installation of Baits for Virus/Worms Attacks:**

With the continuous rise in cybercrime cases, the government needs to prepare new strategies like baits planting in cyberspace for virus or worms attack. A proposal relating to it is being considered by the department of IT (DIT) which has signed MoUs with Microsoft and McAfee. The technology for creating such baits may lead to uneven traffic pattern in internet. The continuous attempted patterns will be analyzed to raise warnings without any potential damage.

The team of Wake Forest University in North Caronia[430] with Pacific Northwest National Laboratory (PNNL)[431] worked together on "swarming intelligence"[432] the idea being to prepare digital ants army to combat with cyber viruses and worms and prevent them from making any losses in advance.

24. **Guidelines for Social Networking Sites:**

Generally, the social networking sites, such as, Facebook, Instagram, Twitter, etc., connects the masses and bring friends closer with each other but they also have ruined the image of various users who were trapped through fake accounts and lands up in cyber frauds. The circulation of fake news, photos and videos is just regular business on the social media. After country wide lockdown during spread of pandemic in India, the social networking sites has been on the rise. It is suggested that certain general guidelines are to be prepared to keep a check on the validity of any posts spreading across internet and prevent any fake news from being viral over social networking sites.

25. **Transparency in appointments under Information Technology Act, 2000:**

The former Justice Rajesh Tandon of Cyber Regulations Appellate Tribunal (CRAT)[433] has mentioned the provisions relating to appointments as 'unreasonable' retiring age of presiding officer and undue delay in appointments. Under the IT Act, the head of a tribunal is need be either High Court judge or member of Indian Legal Services or holds Grade I officer post for at least 3 years. His term has been limited for 5 years or 65 years of age provided under Section 51(1) of IT Act, 2000[434]. Since July 2011, the chairmanship of Cyber Appellate Tribunal remained vacate for five years. Due to lack of

[430] Wake Forest University, , WAKE FOREST UNIVERSITY , https://www.wfu.edu/ (last visited Jul 29, 2020).
[431] Pacific Northwest National Laboratory | PNNL, , https://www.pnnl.gov/ (last visited Jul 29, 2020).
[432] Swarming Intelligence of 1-Trailer Systems, , RESEARCHGATE, https://www.researchgate.net/publication/300113325_Swarming_Intelligence_of_1-Trailer_Systems (last visited Jul 29, 2020).
[433] Chapter 10: The Cyber Appellate Tribunal, , INFORMATION TECH. LAW (2014), *Supra* note 396.
[434] Section 51: Term of office, conditions of service etc of Chairperson and Members, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-51-term-of-office-conditions-of-service-etc-of-chairperson-and-members/ (last visited Jul 29, 2020).

chairman, no bench assembled or hear the cases which resulted in plethora of pending cases. A reasonable change is suggested to enhance more transparency for the appointments as the number of disputes and problems between consumer and platforms like banks, apps and online intermediaries is consistently going up.

26. **Requirement for expert training of officials investigating Cybercrimes:**

One of the important reason behind escape of cyber criminals from legal hands is that judicial officer, lawyers and investigating officer is not fully equipped or trained to deal with Information Technology related matters. According to Section 78 of IT Act, 2000[435], no officer below the rank of Deputy Superintendent of Police (DSP) can investigate the cyber related offences. But, despite of massive 457% increase in cybercrime cases in India, in past few years, one in every five police officers confessed they don't have sufficient training, devices and technology to investigate into cybercrime cases. Many police officers confessed in front of court that they don't possess required knowledge to investigate cyber related offences. It is suggested that proper means of equipment and training to be provided to investigating officers to control this rising cases.[436]

27. **Critical review of ISPs Licenses:**

In India, the Department of Telecommunications (DoT)[437] provides licenses to Internet Service Providers (ISP)[438] but still there are various service providers operating illegally without license. So, it is crucial to timely review the licenses provided to ISPs and strict action to be taken against illegally operating ISPs. In one of the crucial case, UP-ATS worked with the Department of telecommunication and traced the criminal movement of six illegal internet service providers, active without a legal license, they were snatched

[435] Section 78: Power to investigate offences, , INFORMATION TECH. LAW (2014), https://www.itlaw.in/section-78-power-to-investigate-offences/ (last visited Jul 29, 2020).

[436] Digitisation worry: Cyber Appellate Tribunal, which looks into cybercrime, has been headless for five years | India News,The Indian Express, https://indianexpress.com/article/india/cyber-appellate-tribunal-chiefs-post-lying-vacant-since-last-five-years-4426644/ (last visited Jul 29, 2020).

[437] Department of Telecommunications | Ministry of Communication | Government of India, , https://dot.gov.in/ (last visited Jul 29, 2020).

[438] What is an Internet Service Provider (ISP)? - Definition from Techopedia, , https://www.techopedia.com/definition/2510/internet-service-provider-isp (last visited Jul 29, 2020).

from areas of Noida, Greater Noida, and Ghaziabad. They allegedly aiding the Anti-National groups creating riots and supplying illegal arms across the country.[439]

28. **Requirement of anti-hijacking software:**

There are various problems highlighted due to online hijacking in the cyberspace. Almost all the activities are based on the Information and Communication Technology due to the use of mobile phones, computers, internet etc., and unknown redirections from websites may raise security concerns of the user. Therefore, it is suggested to adopt software to eliminate hijacking of systems and enhance the security of delicate systems. Moreover, in order to avoid cyber-attacks from foreign countries, anti-hijacking software needs to be used for enhancing the personal security from outside.

29. **Analyze the recommendations of Malimath Committee on reforms in Criminal Justice System:**

The recommendations of Malimath Committee on reforms in Criminal Justice System provided several suggestions, few among them relating to computer crime mentioned as:

i. **Investigation:** There should be installation of special cyber squad in every state crime branch of India.

ii. **Network Intelligence:** The institutionalization of criminal intelligence branch and the main object of such body is to collect, extract, analyze and disseminate the potential information regarding active criminal groups involved in cybercrimes. They would possess the systematic digital database, providing access to the Central Crime Agencies and all the State Police Cyber Forensics.

iii. **Training the Officers:** the committee highly emphasized to the recommendation to provide required facilities for the practice and training of modern areas, such as, Forensic Accountancy and Information Technology relating to cybercrimes.

[439] Raids on illegal internet service providers in Noida and Ghaziabad, 6 held, , HINDUSTAN TIMES (2017), https://www.hindustantimes.com/noida/raids-on-illegal-internet-service-providers-in-noida-and-ghaziabad-6-held/story-QwnWWgccHuHAV7ow7sS6WL.html (last visited Jul 29, 2020).

The above mentioned suggestions should be analyzed and applied efficiently as per current needs.[440]

30. **Compulsory Computer Education at Schools, Colleges and Offices:**

The understanding of basic cyber technicalities and laws should be taught at every level, where the access of computer and internet usage is high. It is to increase the computer awareness among the masses.

At this final juncture, it can be concluded that the advent of Internet in this present century has highly influenced every areas of human beings. No one can think about a world without the use of technical devices and internet. It should be the top priority to preserve the technology for development and prosperity of the society and to avoid its misuse for any criminal activities. The ease at which the information and data flows from the internet without any border barriers, there are chance of their exploitation by cyber criminals, which may create problems for law enforcement agencies at national as well as international level. Therefore, there should be proper due-diligence and caution while providing any information online.

[440] K. Deepalakshmi, *The Malimath Committee's recommendations on reforms in the criminal justice system in 20 points*, THE HINDU, January 17, 2018, https://www.thehindu.com/news/national/the-malimath-committees-recommendations-on-reforms-in-the-criminal-justice-system-in-20-points/article22457589.ece (last visited Jul 29, 2020).

BIBLIOGRAPHY

PRIMARY SOURCES

LIST OF INDIAN STATUTES:

Indian Penal Code, 1860

Indian Evidence Act, 1872.

The Telegraph Act, 1885.

Constitution of India, 1950.

Copyright Act, 1957.

Criminal Procedure Code, 1973.

Trademark Act, 1999.

Information Technology Act, 2000.

The Information Technology (Amendment) Act, 2008.

LIST OF INTERNATIONAL STATUTES:

United Kingdom:

Computer Misuse Act, 1990.

Data Protection Act, 1998.

Computer Police & Justice Act, 2006.

United States of America:

California's Penal Code, 1872.

United States Federal Criminal Code, 1970.

The Computer Fraud and Abuse Act, 1986.

US Patriot Act, 2001.

Canada:

Criminal Code of Canada, 1985.

Council of Europe Convention on Cyber Crime, Canada 2003.

Australia:

Cyber Crime Act, 2001.

The Criminal Code Act, 1995.

Germany:

Federation Data Protection Act, 1990.

Telecommunications Act, 1997.

Federal Data Protection Act, 2002.

France:

France Council of European Directives, 1958.

French Intellectual Property Code, 1992.

Spain:

Spanish Penal Code, 1870.

Philippines:

Philippines E-commerce Act, 2000.

Sri Lanka:

Computer Crime Act, 2007.

Bangladesh:

Bangladesh Cyber Crime Act, 2004.

Pakistan:

Pakistan Cyber Crime (Prevention of Electronic Crimes) Bill, 2007.

Cyber Crime (Prevention of Electronic Crimes) Act, 2016.

LIST OF INTERNATIONAL BODIES AND CONVENTIONS:

The Paris Convention, 1883.

The Berne Convention, 1886.

General Agreement on Tariff and Trade (GATT), 1947.

The United States Commission on International Trade Law (UNCITRAL), 1966.

The World Intellectual Property Organisation (WIPO), 1970.

The World Trade Organisation (WTO), 1995.

Trade Related aspect of Intellectual Property Rights (TRIPS), 1995.

WIPO Copyright Treaty, 1996.

Internet Corporation for Assigned Names and Numbers (ICANN), 1998.

SECONDARY SOURCES

LIST OF IMPORTANT BOOKS:

Jaishankar, K. (ed.) Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour (New York: CRC Press/Taylor Francis, 2014).

Jonthan Rosenoer, Cyber Law, Springer, New York, (1997).

Chris Reed & John Angel, Computer Law, OUP, New York, (2007).

Vasu Deva, Cyber Crimes and Law Enforcement, Commonwealth Publishers, New Delhi, (2003).

Jewkes, Y. and M. Yar (eds.) Handbook of Internet Crime (Cullompton: Willan Publishing, 2010)

Lloyd, I, Information Technology Law, Oxford University Press Blackstone's Statutes on IT and E-Commerce, Oxford University Press.

Verma S, K, Mittal Raman, Legal Dimensions of Cyber Space, Indian Law Institute, New Delhi, (2004)

Sudhir Naib, The Information Technology Act, 2005: A Handbook, OUP, New York, (2011)

Justice Yatindra Singh, Cyber Laws, Universal Law Publishing Co, New Delhi, (2012).

S. R. Bhansali, Information Technology Act, 2000, University Book House Pvt. Ltd., Jaipur (2003).

Taylor, R. W., E. J. Fritsch and J. Liederbach, Digital Crime and Digital Terrorism (New Jersey: Prentice Hall Press, 2014, 3rd ed.)

Yar, M. Cybercrime and Society (London: Sage, 2013, 2nd ed.)

John R. Vacca, Computer Forensics: Computer Crime Scene Investigation (2008).

Laurence Barton, Crisis in Organizations II (2 edition ed. 2000).

Major Suresh Goel, Crisis Management: Master the Skills to Prevent Disasters (2009).

Steven Fink & American Management Association, Crisis Management: Planning for the Inevitable (1986).

Caywood, Handbook of Strategic Public Relations and Integrated Communications (2004).

Daryl Conner, managing at the Speed of Change: How Resilient Managers Succeed and Prosper where Others Fail (1993).

Dan Pyle Millar & Robert L. Heath, Responding to Crisis: A Rhetorical Approach to Crisis Communication (2003).

H. L. A. Hart, Herbert Lionel Adolphus Hart & Leslie Green, The Concept of Law (2012).

The handbook of strategic public relations & integrated communications, (Clarke L. Caywood ed., 1997).

W. Brian Arthur, The Nature of Technology: What It Is and How It Evolves (Reprint edition ed. 2011).

LIST OF IMPORTANT JOURNALS AND ARTICLES:

Burkiewicz, Ł., Knap-Stefaniuk, A. (2020). Modern Managers and Cultural Diversity in Workplace. IN: Education Excellence and Innovation Management: A 2025 Vision to Sustain Economic Development during Global Challenges. The 35th IBIMA Conference on 1-2 April, 2020 Seville, Spain. 7474-7483, ResearchGate, https://www.researchgate.net/publication/342903036_Burkiewicz_L_Knap-Stefaniuk_A_2020_Modern_Managers_and_Cultural_Diversity_In_The_Workplace_IN_Education_Excellence_and_Innovation_Management_A_2025_Vision_to_Sustain_Economic_Development_during_Global (last visited Jul 23, 2020)

Dealing with the Crisis: Taking Stock of the Global Policy Response ResearchGate, https://www.researchgate.net/publication/228125690_Dealing_with_the_Crisis_Taking_Stock_of_the_Global_Policy_Response (last visited Jul 23, 2020)

Learning from Crisis: A Framework of Management, Learning and Implementation in Response to Crises ResearchGate, https://www.researchgate.net/publication/40823576_Learning_from_Crisis_A_Framework_of_Management_Learning_and_Implementation_in_Response_to_Crises (last visited Jul 25, 2020)

ROLE AND IMPACT OF DIGITAL FORENSICS IN CYBER CRIME INVESTIGATIONS, https://www.researchgate.net/publication/331991596_ROLE_AND_IMPACT_OF_DIGITAL_FORENSICS_IN_CYBER_CRIME_INVESTIGATIONS (last visited Jul 28, 2020)

Strategic Environmental Scanning: An Approach for Crises Management ResearchGate, https://www.researchgate.net/publication/318699538_Strategic_Environmental_Scanning_an_Approach_for_Crises_Management (last visited Jul 24, 2020)

Swarming Intelligence of 1-Trailer Systems ResearchGate, https://www.researchgate.net/publication/300113325_Swarming_Intelligence_of_1-Trailer_Systems (last visited Jul 29, 2020)

Hacking and cybercrime ResearchGate, https://www.researchgate.net/publication/228705030_Hacking_and_cybercrime (last visited Jul 25, 2020)

Plan for emergencies ResearchGate, https://www.researchgate.net/publication/40959374_Plan_for_emergencies (last visited Jul 23, 2020)

5 Steps for Conducting Computer Forensics Investigations | Norwich University Online, https://online.norwich.edu/academic-programs/resources/5-steps-for-conducting-computer-forensics-investigations (last visited Jul 28, 2020)

Bertrand Robert & Chris Lajtha, A New Approach to Crisis Management, 10 Journal of Contingencies and Crisis Management 181–191 (2002), https://onlinelibrary.wiley.com/doi/abs/10.1111/1468-5973.00195 (last visited Jul 23, 2020)

Atal Innovation Mission | NITI Aayog, https://niti.gov.in/aim (last visited Jul 23, 2020)

Causes of CyberCrime and Preventive Measures Krazytech, https://krazytech.com/technical-papers/cyber-crime (last visited Jul 26, 2020)

Kerstin Eriksson & Allan McConnell, Contingency planning for crisis management: Recipe for success or political fantasy? 30 Policy and Society 89–99 (2011), https://doi.org/10.1016/j.polsoc.2011.03.004 (last visited Jul 25, 2020)

Gordon L. Lippitt & Warren H. Schmidt, Crises in a Developing Organization, Harvard Business Review November 1967, Nov. 1, 1967, https://hbr.org/1967/11/crises-in-a-developing-organization (last visited Jul 25, 2020)

Uriel Rosenthal Bert Pijnenburg, Crisis Management and Decision Making: Simulation Oriented Scenarios, 2.

Ali Reza Nojoumi et al., Crisis Management Arising from Technological Risks and its Models in South Pars: A Systematic Review, 10 (2015)

Crisis Management Model, https://www.managementstudyguide.com/crisis-management-model.htm (last visited Jul 29, 2020)

Thierry C. Pauchant & Ian I. Mitroff, Crisis management: Managing paradox in a chaotic world, 38 Technological Forecasting and Social Change 117–134 (1990), http://www.sciencedirect.com/science/article/pii/004016259090034S (last visited Jul 23, 2020)

Paul Shrivastava, Crisis theory/practice: towards a sustainable future, 7 Industrial & Environmental Crisis Quarterly 23–42 (1993), https://www.jstor.org/stable/26162560 (last visited Jul 24, 2020)

Digitisation worry: Cyber Appellate Tribunal, which looks into cybercrime, has been headless for five years The Indian Express, https://indianexpress.com/article/india/cyber-appellate-tribunal-chiefs-post-lying-vacant-since-last-five-years-4426644/ (last visited Jul 29, 2020)

Dave Karpinsky, Discovery of Electronic Evidence Allowable, 9 (2006)

Robert R. Ulmer, Effective Crisis Management through Established Stakeholder Relationships: Malden Mills as a Case Study, Management Communication Quarterly (2016), https://journals.sagepub.com/doi/10.1177/0893318901144003 (last visited Jul 24, 2020)

Christine M. Pearson & Ian I. Mitroff, From Crisis Prone to Crisis Prepared: A Framework for Crisis Management, 7 The Executive 48–59 (1993), https://www.jstor.org/stable/4165107 (last visited Jul 24, 2020)

Here’s Why Top Indian Companies Are Switching to the Paperless Route – My Blog, https://www.tyrustech.com/blog/heres-why-top-indian-companies-are-switching-to-the-paperless-route/ (last visited Jul 26, 2020)

How to build an effective information security risk management program https://blog.netwrix.com/, https://blog.netwrix.com/2018/08/02/how-to-create-an-effective-information-security-risk-management-program/ (last visited Jul 24, 2020)?

How to Create a Social Media Crisis Management Plan [Free Template], https://blog.hubspot.com/service/social-media-crisis-management (last visited Jul 23, 2020)?

Identifying A Crisis and Managing It Effectively Melissa Agnes - Crisis Management Keynote Speaker, https://melissaagnes.com/identifying-a-crisis-and-managing-it-effectively/ (last visited Jul 25, 2020)

Ulrich Sieber, International cooperation against terrorist use of the internet, Vol. 77 Revue internationale de droit penal 395–449 (2006), https://www.cairn.info/revue-internationale-de-droit-penal-2006-3-page-395.htm (last visited Jul 25, 2020)

James M. McCormick, International Crises: A Note on Definition, 31 The Western Political Quarterly 352–358 (1978), https://www.jstor.org/stable/447735 (last visited Jul 23, 2020)

Learning in a Time of Crisis FSG, https://www.fsg.org/blog/learning-time-crisis (last visited Jul 25, 2020)

Lerbinger O 1997 The crisis manager Facing risk and responsibility Mahwah NJ | Course Hero, https://www.coursehero.com/file/p52an47g/Lerbinger-O-1997-The-crisis-manager-Facing-risk-and-responsibility-Mahwah-NJ/ (last visited Jul 23, 2020)

Norman R. Augustine, Managing the Crisis You Tried to Prevent, Harvard Business Review November–December 1995, Nov. 1, 1995, https://hbr.org/1995/11/managing-the-crisis-you-tried-to-prevent (last visited Jul 25, 2020)

Mode and Manners of Committing Cyber Crime Information Technology Essay, https://www.ukessays.com/essays/information-technology/mode-and-manners-of-committing-cyber-crime-information-technology-essay.php (last visited Jul 25, 2020)

Need for a uniformly enabled ICT for the Indian Judiciary, https://www.barandbench.com/columns/need-for-an-ict-uniformly-enabled-indian-judiciary (last visited Jul 27, 2020)

New Cyber Warning: ISIS or Al-Qaeda Could Attack Using 'Dirty Bomb,' https://www.forbes.com/sites/zakdoffman/2019/09/13/cyber-dirty-bomb-terrorist-threat-is-real-warns-us-cyber-general/#1a9d78c5679f (last visited Jul 25, 2020)

Organizational Environment | Types of Environment - Roarwap, https://www.roarwap.com/business-environment/organizational-environment/ (last visited Jul 23, 2020)

Out of the Crisis | The MIT Press, https://mitpress.mit.edu/books/out-crisis (last visited Jul 24, 2020)

PDCA Cycle - What is the Plan-Do-Check-Act Cycle? | ASQ, https://asq.org/quality-resources/pdca-cycle (last visited Jul 24, 2020)

Pepsi's Crisis Response: The Syringe Scare: PRSA, https://apps.prsa.org/SearchResults/view/6BW-9412B04/0/Pepsi_s_Crisis_Response_The_Syringe_Scare (last visited Jul 23, 2020)

Philip Crosby: Contributions to The Theory of Process Improvement and Six Sigma |, https://www.shmula.com/philip-crosby-contributions-to-the-theory-of-process-improvement-and-six-sigma/27873/ (last visited Jul 24, 2020)

PR Crisis Management Lessons from the Nestlé Maggi Noodle Controversy glean.info, https://glean.info/pr-crisis-management-lessons-from-the-nestle-maggi-noodle-controversy/ (last visited Jul 23, 2020)

Prevention of Electronic Crimes Ordinance 2007 An Ordinance-Online Jounalism-Lecture Handouts - Docsity, https://www.docsity.com/en/prevention-of-electronic-crimes-ordinance-2007-an-ordinance-online-jounalism-lecture-handouts/170656/ (last visited Jul 28, 2020)

Raids on illegal internet service providers in Noida and Ghaziabad, 6 held Hindustan Times, https://www.hindustantimes.com/noida/raids-on-illegal-internet-service-providers-in-noida-and-ghaziabad-6-held/story-QwnWWgccHuHAV7ow7sS6WL.html (last visited Jul 29, 2020)

Recognition in a time of crisis | HRD Australia, https://www.hcamag.com/au/specialisation/reward-recognition/recognition-in-a-time-of-crisis/220141 (last visited Jul 25, 2020)

Christine M. Pearson & Judith A. Clair, Reframing Crisis Management, 23 The Academy of Management Review 59–76 (1998), https://www.jstor.org/stable/259099 (last visited Jul 23, 2020)

Revised SOP issued for Lawful Interception of Communication, https://pib.gov.in/newsite/PrintRelease.aspx?relid=80829 (last visited Jul 26, 2020)

Risk Issues and Crisis Management: A Casebook of Best Practice, /paper/Risk-Issues-and-Crisis-Management%3A-A-Casebook-of-Regester-Larkin/ced0e7fe4204f8ebca194042d110a222eaba2f01 (last visited Jul 23, 2020)

Taking Stock of Potential Perils: What Could Go Wrong? | Harvard Business Publishing Education, https://hbsp.harvard.edu/product/6419BC-PDF-ENG?Ntt=&itemFindingMethod=Recommendation&recommendedBy=BH658-PDF-ENG (last visited Jul 25, 2020)

Technological Crisis - BCMpedia. A Wiki Glossary for Business Continuity Management (BCM) and Disaster Recovery (DR)., https://www.bcmpedia.org/wiki/Technological_Crisis (last visited Jul 23, 2020)

Stuart Kauffman & William Macready, Technological evolution and adaptive organizations: Ideas from biology may find applications in economics, 1 Complexity 26–43 (1995), https://onlinelibrary.wiley.com/doi/abs/10.1002/cplx.6130010208 (last visited Jul 24, 2020)

Kweku Ewusi-Mensah, The external organizational environment and its impact on management information systems, 6 Accounting, Organizations and Society 301–316 (1981), http://www.sciencedirect.com/science/article/pii/0361368281900106 (last visited Jul 23, 2020)

The Four Stages of a Crisis Management Essay, https://www.ukessays.com/essays/management/the-four-stages-of-a-crisis-management-essay.php (last visited Jul 23, 2020)

The Information Technology (Amendment) Act, 2008 – The Internet Democracy Project, https://internetdemocracy.in/laws/the-information-technology-amendment-act-2008/ (last visited Jul 29, 2020)

K. Deepalakshmi, The Malimath Committee's recommendations on reforms in the criminal justice system in 20 points, The Hindu, Jan. 17, 2018, https://www.thehindu.com/news/national/the-malimath-committees-recommendations-on-reforms-in-the-criminal-justice-system-in-20-points/article22457589.ece (last visited Jul 29, 2020)

The Stages of Crisis: Understanding the crisis management lifecycle, https://www.noggin.io/blog/the-stages-of-crisis-understanding-the-crisis-management-lifecycle (last visited Jul 23, 2020)

Ian I. Mitroff et al., The structure of man-made organizational crises, 33 Technological Forecasting and Social Change 83–107, https://www.academia.edu/23876994/The_structure_of_man-made_organizational_crises (last visited Jul 24, 2020)

What is a computer worm and how does it work? https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html (last visited Jul 25, 2020)

What is a Denial of Service (DoS) Attack? LIFARS, https://lifars.com/2020/03/what-is-a-denial-of-service-dos-attack/ (last visited Jul 27, 2020)

What is a Salami Attack? Aj Maurya. An Engineer., https://ajmaurya.wordpress.com/2014/03/27/what-is-a-salami-attack/ (last visited Jul 25, 2020)

What is a Trojan Virus? www.kaspersky.co.in, https://www.kaspersky.co.in/resource-center/threats/trojans (last visited Jul 25, 2020)

What is an Internet Service Provider (ISP)? - Definition from Techopedia, https://www.techopedia.com/definition/2510/internet-service-provider-isp (last visited Jul 29, 2020)

What is the Crisis Management Model? Definition & examples toolshero, https://www.toolshero.com/management/crisis-management-model/ (last visited Jul 24, 2020)

What is web-jacking? | Karnika Seth - Cyberlawyer & Expert, https://www.karnikaseth.com/what-is-web-jacking.html (last visited Jul 25, 2020)

LIST OF IMPORTANT WEBSITES AND MEDIA:

Department of Information Technology under Ministry of Electronics & IT, India, https://www.meity.gov.in/

Cyber Terrorism, https://www.terrokrismanswers.com/terrorism

Crime Research, http://www.crime-research.ru/news/

Treaties and Conventions, http://conventions.coe.int/Treaty/en/Treaties/Html/185.html

Cybercrime India, http://www.cyberkeralam.in.888/berket/Common/Schemes.jsp

Crime Library, www.crimelibrary.com

Cyber Laws, www.cyber.law.harvard.edu

Cyber Law Reports, www.cyberlawassociation.com

Cybercrimes, www.cyberattack.in

Cyber Security, www.windowsecurity.com

Cybercrime Cases, www.cybercases.blogspot.com

Wikipedia, www.wikipedia.com

ANNEXURE-I

QUESTIONNAIRE

1. Name :

2. Age :

3. Gender:

4. Education Qualification :

5. Organization :

6. Area of Employment : A) Software Design and Development [ ]

B) Hardware Development [ ]

C) I.T.E.S. [ ]

D) B.P.O [ ]

E) Banks and Financial Institutions [ ]

F) Other

7. Are you aware of Information Technology (IT) Act, 2000?

Yes [ ]

No [ ]

8. Section 43 of IT Act states about the penalty for the damage to computer, computer systems etc., i.e., illegal access to computer systems, downloading or copying data, inducing virus attacks on it, damaging the computer, its stored data or network etc., shall be liable to pay by the way of compensation up to Rs. 1 Crore. Do you think that:

A. Adequate and substantial [ ]

B. Should be enhanced [ ]

C. Excessive and should be reduced [ ]

9. Sec.65 of the IT Act provides for punishment for 'Tampering with computer source documents' with imprisonment up to three years or with fine up to Rs. Two lakhs or with both. Do you think that:

A. Adequate and substantial [ ]

B. Should be enhanced [ ]

C. Excessive and should be reduced [ ]

10. ‘Hacking’ is punishable under Sec. 66 of the IT Act with imprisonment up to3 years or with fine of Rs. Two lakhs, or with both. Do you think that:

A. Adequate and substantial [ ]

B. Should be enhanced [ ]

C. Excessive and should be reduced [ ]

11. ‘Publishing of information which is obscene in electronic form' under Sec. 67 of the IT Act with imprisonment up to 10 years or with fine of Rs. Two lakhs, or with both. Do you think that:

A. Adequate and substantial [ ]

B. Should be enhanced [ ]

C. Excessive and should be reduced [ ]

12. ‘Breach of confidentiality and privacy’ under Sec. 72 of the IT Act with imprisonment up to 2 years or with fine of Rs. One lakh, or with both. In addition to this, it is proposed to amend this clause and bring about by way of compensation for breach of confidentiality; capturing or broadcasting an image of a person without consent, to a sum of Rs. 25 Lakhs Do you think that this is:

A. Adequate and substantial [ ]

B. Should be enhanced [ ]

C. Excessive and should be reduced [ ]

13. As provided under Sec.85 ‘offences by companies’, all persons, who were in charge of, and were responsible to, the company for the conduct of business at the time of the breach of any provision of the I T Act shall be liable to be proceeded against and punished accordingly; with the exception of any one proving beyond reasonable doubt that the incident took place without his knowledge or that they had exercised “due Diligence” to prevent it. Do you agree with this clause?

Yes [ ]

No [ ]

14. Do you think the IT Act 2000 is capable of preventing cyber Crime?

Yes [ ]

No [ ]

15. Cybercrimes are committed beyond international boundaries. Do you think that an international law, rather than a law specific to a nation’s jurisdiction is more beneficial to face future challenges such as international fraud, money laundering and terrorism?

Yes [ ]

No [ ]

16. Do you think that some aspects of intellectual property right protection, trademark and copyright infringements should also be incorporated within IT Act?

Yes [ ]

No [ ]

17. Have come across any cybercrime during your occupation?

Yes [ ]

No [ ]

18. If you come across a cybercrime in your line of work how would you respond to it?

A. Inform Superior personnel within the organization [ ]

B. Inform the Police [ ]

C. React to it on your own initiative [ ]

D. Ignore it [ ]

19. Does your organization have a specific protocol in preventing such instances?

Yes [ ]

No [ ]

20. Should every organization have its own cyber security system?

Yes [ ]

No [ ]

21. Should law alone particularly the government worry about cybercrime?

Yes [ ]

No [ ]

22. Most of the cybercrime is by insiders or disgruntled ex-employees do you agree with this?

Yes [ ]

No [ ]

23. Do you think that India should have a campaign to educate and to raise awareness of responsibility among computer users:

Yes [ ]

No [ ]

24. Which do you think is the most common loss due to cybercrime?

a. Money. [ ]

b. Service Quality. [ ]

c. Credibility and reputation. [ ]

d. Competitive Edge [ ]

f. All of the above. [ ]

25. Which of these cybercrimes that are most frequently encountered by you?

A. E-mail bombing [ ]

B. Data diddling [ ]

C. Salami attacks [ ]

D. Virus/Worm Attacks [ ]

E. Logic bombs [ ]

F. Trojan attacks [ ]

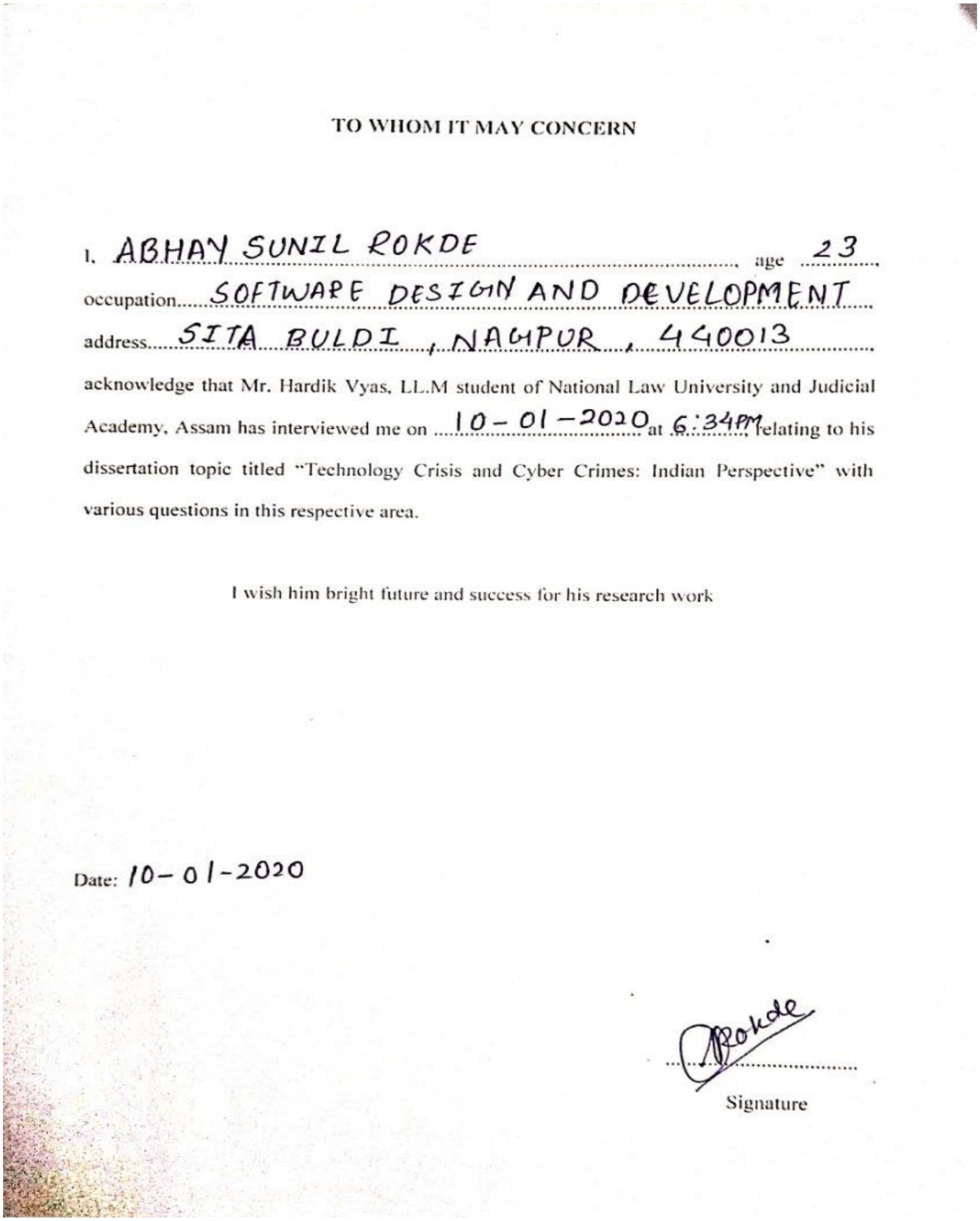
G. Internet time thefts [ ]

H. Web jacking [ ]

I. Obscene Mail [ ]

ANNEXURE-II

CERTIFICATES



TO WHOM IT MAY CONCERN

I, ABHAY SUNIL ROKDE, age 23

occupation SOFTWARE DESIGN AND DEVELOPMENT

address SITA BULDI , NAGPUR , 440013

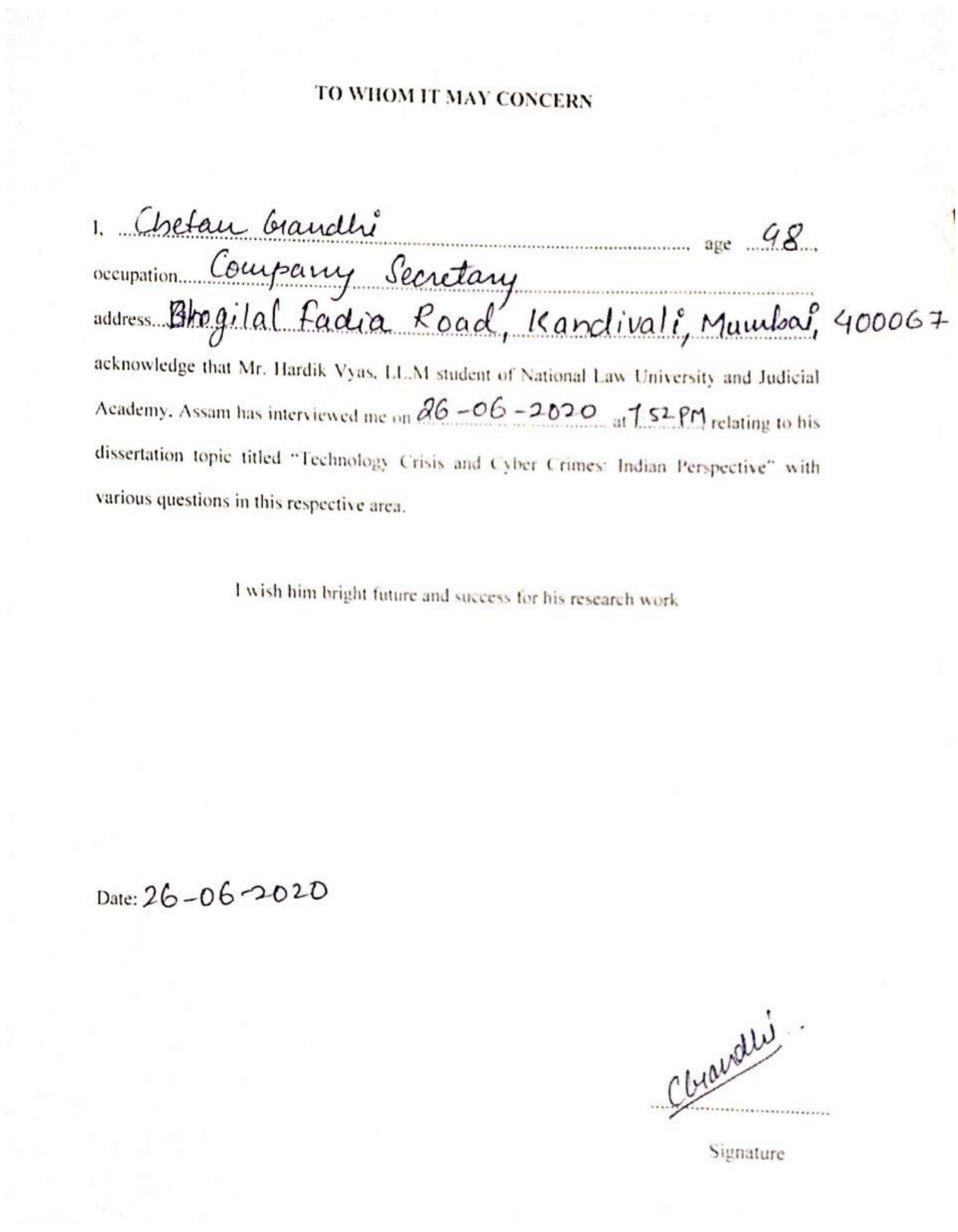
acknowledge that Mr. Hardik Vyas, LL.M student of National Law University and Judicial Academy, Assam has interviewed me on 10-01-2020 at 6:34PM relating to his dissertation topic titled "Technology Crisis and Cyber Crimes: Indian Perspective" with various questions in this respective area.

I wish him bright future and success for his research work

Date: 10-01-2020

Rokde

Signature



TO WHOM IT MAY CONCERN

I, Chetan Gandhi age 98,
occupation Company Secretary
address Bhogilal Fadia Road, Kandivali, Mumbai, 400067

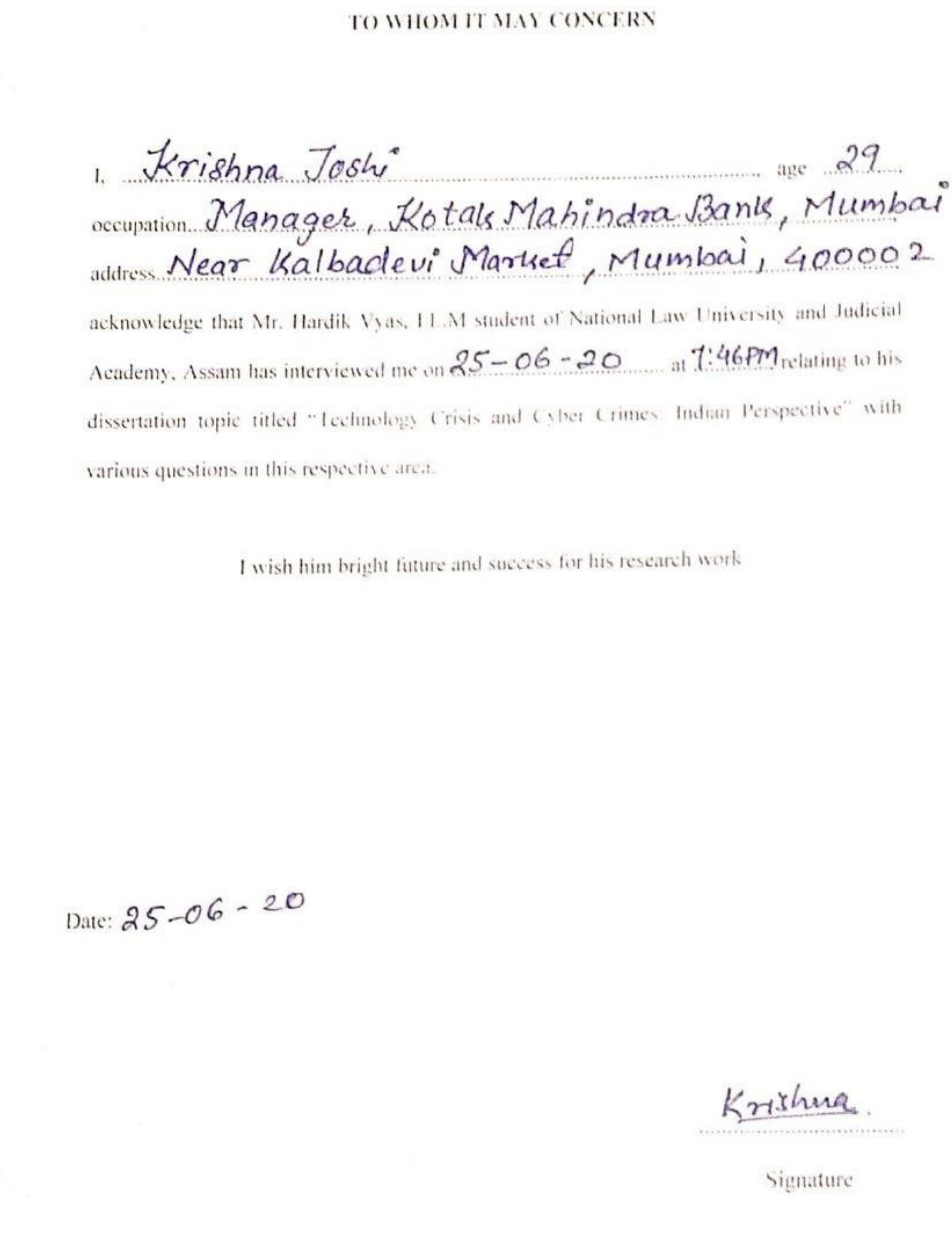
acknowledge that Mr. Hardik Vyas, LL.M student of National Law University and Judicial Academy, Assam has interviewed me on 26-06-2020 at 7 52 PM relating to his dissertation topic titled "Technology Crisis and Cyber Crimes: Indian Perspective" with various questions in this respective area.

I wish him bright future and success for his research work

Date: 26-06-2020

Gandhi

Signature



TO WHOM IT MAY CONCERN

I, Krishna Joshi age 29
occupation Manager, Kotak Mahindra Bank, Mumbai
address Near Kalbadevi Market, Mumbai, 400002

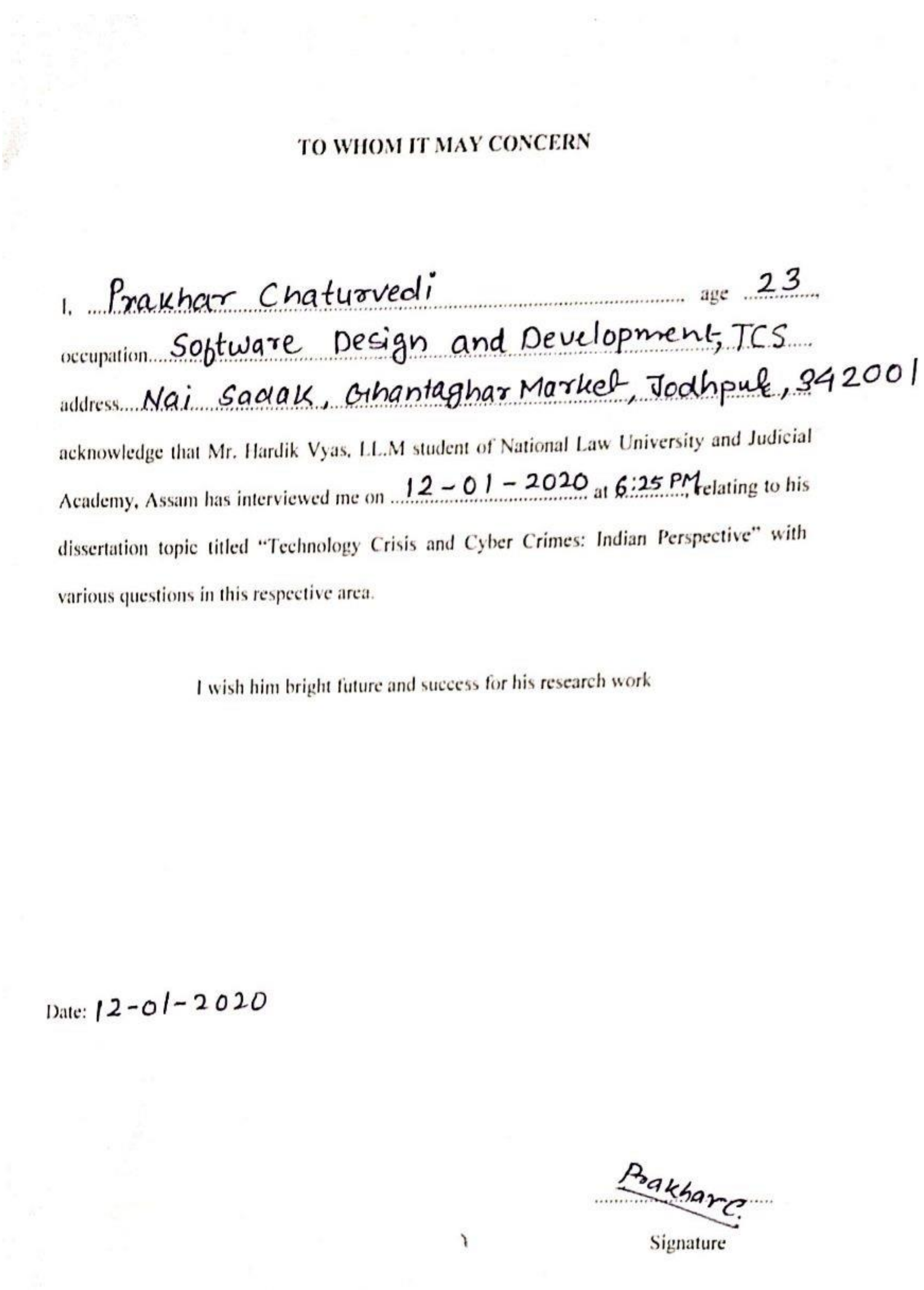
acknowledge that Mr. Hardik Vyas, LL.M student of National Law University and Judicial Academy, Assam has interviewed me on 25-06-20 at 7:46PM relating to his dissertation topic titled "Technology Crisis and Cyber Crimes: Indian Perspective" with various questions in this respective area.

I wish him bright future and success for his research work

Date: 25-06-20

Krishna.

Signature



TO WHOM IT MAY CONCERN

I, Prakhar Chaturvedi age 23

occupation Software Design and Development, TCS

address Nai Sadak, Ghantaghar Market, Jodhpur, 342001

acknowledge that Mr. Hardik Vyas, LL.M student of National Law University and Judicial Academy, Assam has interviewed me on 12 - 01 - 2020 at 6:25 PM relating to his dissertation topic titled "Technology Crisis and Cyber Crimes: Indian Perspective" with various questions in this respective area.

I wish him bright future and success for his research work

Date: 12-01-2020

Prakhar C.

Signature

LIST OF TABLES

LIST OF FIGURES