Journal of Advances and Scholarly Researches in Allied Education
Vol. 20, Issue No. 4, October-2023, ISSN 2230-7540

Cyber Security Awareness and Prevention Strategies

Rajat Bhatia[1]*, Dr. Aparna Soni[2]

[1] Research Scholar, University of Technology, Jaipur, Rajasthan, India

[2] Associate Professor, Department of Management, University of Technology, Jaipur, Rajasthan, India

Abstract - The use of a computer as a tool can be involved in the following forms of unlawful behaviour: financial crimes, sale of illicit things, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, and cyber stalking. Computers may also be utilised to participate in online gambling games such as poker and blackjack. On the other hand, the computer could be a target for illegal activity in the following scenarios: unauthorised access to the computer, computer system or computer networks, theft of information contained in electronic form, e-mail bombing, Salami attacks, logic bombs, Trojan attacks, Internet time thefts, web jacking, theft of computer system, and physically damaging the computer system. The internet has emerged as the most vital piece of physical infrastructure in this modern era. There has never been a time in the history of mankind and there has never been an innovation that has generated such great and substantial changes in the economics of the globe, personal communication, and every sector that pertains to our age as the information age has. The internet provides instant communication between any computers that are linked to it, point-to-point communication, and offers an expanding number of private and public communication options. The Internet is a worldwide resource that connects millions of users using a standardised set of protocols. These protocols are a form of communication that is mutually agreed upon between the parties involved.

Keywords - Cyber, Security, Awareness, Prevention, Strategies

----------X----------

INTRODUCTION

Definitions and Categories of Online Criminal Activity

The ways in which people commit crimes are undergoing profound shifts as a direct result of the continuous development of the human intellect. Criminals are growing more and more savvy on a daily basis, and they are employing their intelligence in this setting to commit crimes and get away without being apprehended. When personal computers first became widely available, few imagined that they would one day be used as a tool or an inspiration for criminal activity. Charles Babbage, who is often regarded as the inventor of the computer, probably never would have imagined that the invention he was gifting to the world would one day play a role in the commission of crimes or otherwise negatively impact society. When we talk about anything being a cyber crime, we are usually referring to a wrongdoing that involves a computer system in some way. The term "cyber crime" was given to an incorrect category of illegal activity. This phrase does not appear to have any definition in any of the statutes or acts that have been passed or enacted by the Indian Parliament. The idea of committing a crime online is not tremendously dissimilar to the idea of committing a crime in the traditional sense.

Conventional Crime

Criminal behavior is a social and economic phenomena that has existed for as long as human society has been present. It is estimated to have begun about the year 3000 BCE. The concept that we refer to as "crime" is one that is governed by the law and is under its scope. When we talk about a "crime" or a "offence," we imply something along the lines of a "legal infraction that can be followed by a criminal process that may end in punishment." Lord Atkin was quoted as saying, "The criminal quality of an act cannot be identified by reference to any standard but one is the conduct forbidden with penal consequences." "The criminal quality of an act cannot be detected by reference to any standard," Lord Atkin said. "The criminal quality of an act cannot be identified by reference to any standard." This is the defining trait of someone who engages in illicit activity. It is conceivable to define a crime as any behaviour that is followed by an act or omission that is prohibited by law and the violation of which ultimately leads in penal repercussions. One way to

do this is to say that a crime is any behaviour that is associated with breaking the law.

Cyber Crime

Within the world of the internet, the problem of cybercrime is the most recent problem to arise, and it is also possibly the problem that will be the hardest to fix. It is conceivable to describe "cyber crime" as "those species of which genus is the conventional crime and where either the computer is an object or subject of the behaviour that defines crime." This is one definition for "cyber crime," but there are other alternative definitions. Traditional criminal activity might be thought of as the "genus" of "cyber crime." The phrase "cyber crime" refers to any illegal behaviour that involves the use of a computer in some form, whether as a target, an instrumentality, or as a means to accomplish additional criminal activities. This might include using a computer as a tool to commit other crimes. The statement "illegal activity in which the computer is either a tool or target or both" may serve as a good working definition of the word "cyber crime." Alternatively, the phrase "illegal conduct in which the computer is either a tool or target or both" may also suffice. The use of a computer as a tool can be involved in the following forms of unlawful behaviour: financial crimes, sale of illicit things, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, and cyber stalking. Computers may also be utilised to participate in online gambling games such as poker and blackjack. On the other hand, the computer could be a target for illegal activity in the following scenarios: unauthorised access to the computer, computer system or computer networks, theft of information contained in electronic form, e-mail bombing, Salami attacks, logic bombs, Trojan attacks, Internet time thefts, web jacking, theft of computer system, and physically damaging the computer system.

Distinction Between Conventional and Cyber Crime

It would appear that there is no difference between traditional crime and cyber crime given that both types of crime end in some kind of damage being incurred by one of the parties involved. On the other hand, if we do some serious soul-searching, we could come to the conclusion that there is a discernible but incredibly thin line of separation between traditional crime and cybercrime. The defining characteristic is the extent to which the media is involved in instances of cybercrime. "Crime against Individual or Organization by use of Computer is termed as Cyber Crime," is one definition of what constitutes a "cyber crime." Crimes that are carried out within a network environment or on the internet are referred to as cyber crimes.

Cyber Criminals

A person is considered to be an offender or a criminal if they are found guilty of committing a crime or an illegal conduct with the purpose of doing so. In this sense, the term "cyber criminal" refers to any anyone who is guilty of committing a computer crime. Cybercriminals can be youngsters and teenagers between the ages of 6 and 18, they can be members of organised hacking groups, they can be professional hackers or crackers, they can be disgruntled workers, they can defraud, and they can even be psychic people.

Classification of Cyber Crimes

As the scope of cybercrime has grown, it has become essential to examine the ways in which different types of cybercrime might vary in their nature and appearance. As a consequence of this, the many behaviours that have the potential to constitute a criminal offence have been roughly categorised into three primary categories36, which are as follows:

1. Cyber Crimes where computer is used as target.
2. Cyber Crimes where computer is an instrument facilitating the crime; and
3. Cyber crimes where computer is incidental to other crimes.

1. Computer as a target of the Crime :

In this category of cyber crimes, computer is itself a target of the crime. The crimes which are covered under this category are -

I The malicious destruction of computer networks or computer systems.

(ii) The use of sabotage in computer operating systems and software packages.

(iii) The unauthorised acquisition of data or information.

(iv)Theft of intellectual property, including computer software and other forms of intellectual property.

2. The Computer as a Means to Facilitate Criminal Activity: -

The proliferation of microcomputers has led to the development of innovative forms of previously established crimes. This type of criminal activity encompasses a wide range of illegal activities, including, but not limited to, stealing technological equipment, pirating software, and violating the copyright of computer programmes. Another example of this sort of criminal activity involving computers is the illegal sale of duplicate databases. The most notable case in which a computer was used as a tool to commit a cyber crime was the terrorist attack on the Indian parliament on December 13, 2001. The attackers utilised the computer and the Internet in a number of different ways to accomplish the crime. Internet-based communication channels, including as encrypted e-

mail and flash files, are often utilised by criminals all around the world.

International Agencies for Regulating E-Commerce

There are certain international agencies which function to regulate trade and e-commerce at the global level and provide a forum for resolution of disputes and problems by mutual negotiations. The main among them are as follows:

World Trade Organisation (WTO)

At the conclusion of World War II (1939-1945), economists from all over the world convened in Briton Woods, Hampshire, to discuss the possibility of establishing a global organisation with the goals of reestablishing economic order, achieving greater harmony in international trade and tariffs, and resolving issues with the global monetary system. The United States Congress was opposed to the establishment of an International Trade Organization, which meant that the proposal to create such an organisation was ultimately unsuccessful. On the other hand, in 1947, officials from 56 different nations convened once more in Havana to work on developing principles that would enhance and control international commerce. As a direct consequence of this, the contracting nations came together in December 1947 to sign the General Agreement on Tariffs and Trade (GATT). In its early stages, GArr focused on lowering tariffs and increasing commerce between nations; but, it did not initially include a framework for the resolution of trade disputes. The General Agreement on Tariffs and Trade (GATT) held its eighth round in Uruguay in 1986, which resulted in the proposal for the development of the World Trade Organization (WTO). The WTO was intended to deal with the following issues:

1. Trade related IPR's
2. Trade related investment measures
3. Trade related services
4. Agricultural subsidy; and
5. Trade related dispute settlement mechanism.

Provisions Ancillary to Cyber Contraventions

The Controller or any other official designated by him in his behalf has the authority, as stated in Section 28, to investigate any violations that have been committed. It should read as follows:

Power to investigate Contraventions:133

1. Any violation of the provisions of this Act, the rules or regulations adopted thereunder, or any other law that the Controller or any other official authorised by him in his behalf on his behalf must take up for inquiry.

2. The Controller or any other officer authorised by him in his behalf shall exercise the same powers which are conceited on income tax authorities under chapter XII of the Income tax Act, 1961, and shall exercise such powers subject to such limitations laid down under that Act. 2. The Controller or any other officer authorised by him in his behalf shall exercise the like powers which are conceited on income tax authorities under chapter XII of the Income tax Act, 1961.

3. With the permission of the Controller or any officer authorised by him in this behalf or by the Adjudicating Officer, as the case may be, and subject to certain conditions that the parties may specify, Section 63 grants the parties the authority to settle the matter between them by compounding the violation. This must be done with the permission of the Controller.

The concept of private defence:

There is no law in India that expressly addresses the prevention of malware through the use of private defence. Therefore, the existing provisions that are equivalent to one another need to be implemented in a purposeful manner. When it comes to dealing with and combating the use of malware through the employment of private defence, the following sections of the Indian Penal Code, which is a general legislation that deals with offences in India, are of utmost relevance. I Acting in accordance with one's constitutionally protected right to private defence exempts a person from criminal liability under the provisions of Section 96 of the Code. This section acknowledges the self-help concept, which is recognised as being just, fair, and reasonable throughout all of the countries of the globe. (ii) In accordance with the provisions of Section 97 of the Code, every individual possesses the right, subject to the limitations outlined in Section 99, to defend: First, he protects his own body as well as the bodies of anybody else who comes into contact with him from any disease that affects humans. Second: The property, whether it be movable or immovable, of himself or of any other person, against any conduct which is an offence coming within the description of theft, robbery, mischief, or criminal trespass, regardless of whether the act was committed by him or by any other person. This provision recognises that a "third person" has the right, in addition to safeguarding their own property, to protect the property of another individual. Therefore, a selfless person who helps innocent people who have been affected by malware has the right to engage in self-help activities. For instance, a netizen who is an expert in safeguarding computers from viruses may build a software, which has a potential to stop the virus posted on the internet and may launch the same on it. In this scenario, the person who launched the virus cannot say that the third party has no reason to be upset and no right to act against them because they do not have any of those things.

OBJECTIVES OF THE STUDY

1. To study on International Agencies for Regulating E-Commerce
2. To study on Provisions Ancillary to Cyber Contraventions

RESEARCH METHOD

The fundamental goals of data analysis are to manage the information in the appropriate manner, arrive at analytical results that are persuasive, and reject competing hypotheses. When selecting the most appropriate statistical approaches, it is essential to take the following important considerations into account:

Research Design

Data collection is done so that decisions may be made about key issues, records of information can be kept, and information can be communicated to others. Information on "Financial Cyber Crime and its Management" was the primary focus of the data gathering process early on.

Data Collection

The gathering of data for an improvement project often begins in the beginning stages of the project itself, and it is frequently formalised by a data collection Plan, which frequently includes the activity described in the following sentence. Before any data is ever gathered, one of the most critical steps in the process is the activity known as "pre-collection." After the fact, it is occasionally recognised that the worth of their interview material had been underestimated. This is typically the consequence of poor elicitation methods, poor elicitation methodology, and poor selection of both questions and informants. Once the preliminary work has been accomplished in its entirety, the data collection that takes place in the field, whether it be through interviews or some other methods, may be carried out in a controlled, rigorous, and scientific manner. Data collection is done so that decisions may be made about key issues, records of information can be kept, and information can be shared with others. Information on "Financial Cyber Crime and its Management" was the primary focus of the data gathering process early on.

DATA ANALYSIS

The consequences of computer crime penalty for damage of computer, computer system etc. 2

In the event that any individual, without the consent of the computer's owner or any person in charge of the computer network, system, or system administrator:

a) Accesses or secures access to such computer, computer system or computer network;
b) performs a download, copy, or extraction of any data, computer data base, or information maintained or stored on any removable storage medium from such computer, computer system, or computer network;
c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
d) any computer, computer system, or computer network, any data, computer data base, or any other programme housed in such a computer, computer system, or computer network, is damaged, or is caused to be harmed;
e) Disrupts or causes disruption of any computer, computer system or computer network;
f) Denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;
g) Whoever, in violation of the requirements of this Act, rules or regulations issued thereunder, provides any help to any person in order to facilitate access to a computer, computer system, or computer network in violation of the following provisions:
h) 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,
i) He shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.

Explanation For the purposes of this section-

(i). "Computer contaminant" means any set of computer instructions that are designed-

(a). To modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b). By any means to usurp the normal operation of the computer, computer system or computer network:

(ii). The term "computer data base" refers to a representation of information, knowledge, facts, concepts, or instructions in the form of text, image, audio, or video that is being prepared or has been prepared in a formalised manner, or that has been produced by a computer, computer system, or computer network, and is intended for use in a computer, computer system, or computer network;

(iii). "Computer virus" refers to any computer instructions, information, data, or programme that either destroys, damages, degrades, or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data, or instruction is executed or some other event takes place in that

computer resource; "worm" refers to a parasitic organism that replicates itself by inserting its genetic material into other organisms; "trojan horse" refers to a

(iv). "damage" means to obliterate, change, delete, add, add, edit, or reorganise any computer resource using whatever means at one's disposal. 'Computer' is defined as any electronic, magnetic, optical, or other high-speed data processing device or system that performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic, or optical impulses. It also includes all input, output, processing, storage, computer software, or communication facilities that are connected or related to the computer in a computer system or a computer network. 'Computer' can also refer to a network of computers.

Clarifies that "computer system" means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer program, computer instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication controls and other functions.4

Tampering with computer source documents :

Whoever intentionally or knowingly conceals, destroys, or alters any computer source code used for a compute; computer programme, computer system, or computer network, or intentionally or knowingly causes another person to conceal, destroy, or alter any computer source code, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punished with imprisonment for up to three years, a fine that may extend up to two lakh rupees, or both. Explanation: For the purposes of this section, the phrase "computer source code" refers to the listing of programmes, computer consultants, design and layout, and programme analysis of any computer resource in whatever form.

Thus, the essential ingredients of s. 65 are :

1. A person should conceal, destroy or alter or cause another person to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network;

2. the computer source code should be required to be kept or maintained by law for the time being in force;

3. the concealment, destruction or alteration to computer source code should be done intentionally or knowingly.

The source code refers to the programme that was created on the computer, regardless of whether it was written in machine language, assembly language, or high level language. The term "object code" refers to the code that is produced once the "source code" has been translated into machine language by an assembler, a compiler, or a translator. Therefore, the object code is represented by long strings of ones and zeros using the binary number system or the hexadecimal notation of the electrical charges. The object code cannot be seen, felt, or heard, yet its existence cannot be questioned under any circumstances. 14 The entirety of the programming process is included in the definition of the computer source code that is provided by the Act. It consists of computer commands and programming codes (machine, assembly, and high level), design prototypes, flow charts and diagrams, technical documentation, design and layout of the necessary hardware, programme testing details, and other relevant information. The Act is willing to acknowledge computer source code in either physical or palpable form. The preceding section's primary purpose is to safeguard the intellectual property that has been invested in the various computer programmes. It is an effort to provide further legal protection for computer source materials (codes) in addition to the protections already afforded by copyright law.

The source codes of a computer programme can be read by humans, but the object codes can only be understood by computers.

Hacking with computer system -

1. Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in the computer resource of diminishes its value or utility or affects it injuriously by any means, commits hacking.
2. Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.
3. "Computer resources" used in the definition of hacking is defined in section 2 (K) of the Act. It runs as under : Computer resource means computer, computer system or computer network data, computer database or software"18

A Person is said to commit hacking :-

1. When he causes wrongful loss or damage to the public or to any person.

2. by destroying or deleting or altering any information residing in the computer resource or by diminishing its value or utility or affecting it injuriously by any means:

3. With the intention or knowledge that he is likely to cause such wrongful loss or damage to the public or to any person.

According to Section 6(23)19 1860, "Wrongful loss" is defined as the loss of property by unlawful methods by a person who was lawfully entitled to such property. The individual who engages in the illegal activity of hacking is referred to as a hacker. The term "hacking" is also used interchangeably with phrases such as "unauthorised access to computer" and "computer trespass." This is because hacking is a widespread term in common usage. However, in order to be considered hacking in accordance with section 66, it is necessary for additional conditions outlined in the section to be satisfied. Hacking is a type of computer crime that may be done in relation to both tangible and intangible property. Intangible assets comprise information in the form of electrical, magnetic, or optical impulses, whereas physical assets include the hardware components of the computing resource(s). For instance, a computer hard disc is a tangible asset, but it could also store intangible assets in the form of information. Optical storage devices such as CD-R, CD-RW, DVD-R, and DVD-RW are examples of physical assets, but they may also include intangible assets in the form of "optical impulses." Intangible assets will always be a component of tangible assets. Therefore, hacking would involve the destruction or manipulation of a computer resource's physical and/or intangible assets.

The following things have been deemed to be obscene by the court because they lead people whose brains are susceptible to immoral influences to become depraved and corrupt. (2) which conjures up images of a person who is very immoral and libidinous in nature. (3) This is really explicit pornography. (4) that encourages sexual impulses and has a strong propensity to be corrupting because it does. (5) that has a propensity to stimulate sexually immoral ideas. (6) that is within the acceptable range based on the criteria established by our community standards. In a nutshell, the content in question was deemed to be obscene by the Supreme Court in the case of Ranjit Udeshi because it "is likely to deprave and corrupt people whose minds are receptive to influences of this type and into whose hands the book is likely to fall." The Honorable Court went on to rule that "... the obscene matter must be considered by itself and separately to find out whether it is so gross and its obscenity is so decided that it is likely to deprave and corrupt those whose minds are open to influences of this sort and into whose hands the book is likely to fall." The Supreme Court of India, in the case of Chandrakant Kalyandas Kakodar v. State of Maharashtra30, expanded the test of obscenity that had been laid down in the Ranjit Udeshi case by stating that "it is the duty of the Court to consider the obscene matter by taking an overall view of the entire work and to determine whether the obscene passages are so likely to deprave and corrupt those whose minds are open to the influence of As a result, it is clear to see, based on the Chandrakant Kalyandas Kakodkar case, that regardless of how obscene a passage or subject matter might appear to be when viewed in isolation, the passage or subject matter might not be considered obscene when viewed in the context of the entirety of the work. It is possible to determine whether or not a piece of content is obscene by considering the norms of the local community as well as the morals of the modern society. The criterion that is used to establish what constitutes obscene content is whether or not a reasonable and prudent person would consider the work to be obscene when viewed in its entirety.

The spreading of obscene content by any means of communication or publishing it in electronic form is strictly banned. When such a technique "carries with it the serious threat of hurting the sensibilities of an unwilling receiver or to exposing minors," it is considered to be unacceptable. 32 The act of appealing to a shameful or morbid curiosity in sex is what is meant by the term "appeal to prurient interest." It is argued that anything is attractive to the prurient interest in sex if it either creates or encourages an unhealthy concern with sexual matters, displays sexual behaviour in a way that is obviously inappropriate, or both of these things. Cases involving obscenity typically include activities committed in more than one jurisdiction, and pornography sellers can be punished in a state where the material is supplied if they are caught in that state. 33 It is not essential to establish that the defendant had particular knowledge of the destination of each message; this aspect of the case does not need to be proven. Obscenity is a continuing offence, meaning that it is considered a new crime each time it is committed.

Protection against Offences Committed Online

In spite of the fact that the Indian Penal Code and the Information Technology Act contain punitive provisions and preventative measures respectively, it is abundantly clear from a review of the Cybercrime statistics of previous years that there has been no reduction in the crime rate; on the contrary, these statistics are recording a consistent upward trend. Because there are so many new forms of cybercrime appearing, it is necessary to develop improvised investigative and legal methods and abilities in order to deal with them effectively. 62 Because crime statistics contain pertinent data on particular crimes and offenders, they play an important part in the process of formulating preventive crime strategy. This is because the data in crime statistics help criminal law enforcement agencies make the best possible use of the statistics when formulating effective strategy to effectively tackle the issues they face.

The best medicine is always preventative health care. When working with the internet, it is important to practise safe computing habits at all times.

Anyone should include them into their own personal virtual existence.

CONCLUSION

We are currently living through a period of unprecedented change brought about by advances in information technology. First with the invention of computers and subsequently with the development of computer networking, the process of storing information and gaining access to that information has become significantly easier. As a consequence of this, the barriers posed by distance and time were removed from the communication process. The current generation is living in a time where everything is moving at a breakneck speed as a direct result of the rapid growth of technology. Since we are doomed to die if we do not adjust to the shifting conditions in our environment, there is no room for complacency, and there is not even enough time for us to take a breath. The next wave of economic development is being driven in large part by changes in technology. In order to capitalise on that expansion, not only will we need to implement new technologies, but we will also need to adopt new ways of thinking. The last decade of the 20th century saw the rise of information technology as the most prominent kind of technology. This technology has had a transformative impact on the daily lives of people all over the world, to the point that the world may be described as having become a global village. The computer is the engine that is powering the revolution in information technology, and it has found a myriad of applications since its invention. The development of the internet, which represents the most recent innovation in the sector of communication technology, was made possible by the convergence of telecommunication and computer technologies.. In today's modern world, cyberspace is increasingly exerting its influence over every aspect of human endeavour. The internet is bringing about a major and irreversible shift not just in the economic environment but also in the underlying premises upon which enterprises are founded. E-commerce has emerged as a key component of the new electronic economy that has emerged as a result of this transformation of the industrial economy.

REFERENCES

1. Miller LeRoy Roger, Cross B. Frank, The Legal and e-Commerce Environment Business in its Ethical Regulatory and International Setting, (South-Western Thomson Learning, South- Western College Publishing, A Division of Thomson Learning, 2002)
2. Mishra R.C., Cyber Crime: Impact in the new Millennium, (Authorspress Global Network, E-35/103, Jawahar Park, Laxmi Nagar, Delhi-110092, 2002)
3. Nair P.M., Cambating Organised Crime, (Konark Publishers P.Ltd., A- 149, Main Vikas Marg, Delhi- 110092, 2002)
4. Nanda SS and Tewari RK, Forensic Science in India: A Visionfor the Twentyfirst Century, (Select Publishers, New Delhi, 2001)
5. Nigam R.C., Law ofCrime in India Vol. I Principles ofCriminal Law, (Asia Publishing House, Bombay, 1964)
6. Oberoi Sundeep, E-Security and You-Electronic Authentication and Information Systems Security, (Tata Me Graw- Hill Publishing Co Ltd., New Delhi, 2001)
7. Panda D.N., Practical Handbook on The Information TechnologyAct, (Mashbra Industries P Ltd., Saurabh Print-o-Pack, Noida, 2000)
8. Papke Jerry, Bader laura, Cambating Computer Crime- Prevention, Detection and Investigation, (Charrtico Publishing Co. Inc., Me Graw Hills, Inc., 1992)
9. Paranjape N.V., Criminology and Penology, (Central Law Publications, Law Publishers and Book Sellers, 107, Darbhanga Colony, Allahbad, 1996)
10. Peter Carey, Data Protection in the UK, (Blackstone Press Limited, Aldine Place London W128 AA UK, 2000) 55. Pfaffenberger B., Protect Your Privacy On The Internet, (Wiley, 1997)
11. Pfleeger P. Charles, Pfleeger Lawrence Shari, Security in Computing, (Pearson Edition (Singapore) Pvt Ltd., Indian Branch, 482 F.I.E. Patparganj, Delhi110092, 2004)
12. Reed Chris, Computer Law, (Universal Law Publishing Co. Pvt Ltd., New Delhi, 2000) 58. Reed Chris, Internet Law Text andMaterials, (Butterworths Indian, New Delhi, Reed Elsnier, UK Ltd, 2000)

Corresponding Author

Rajat Bhatia*

Research Scholar, University of Technology, Jaipur, Rajasthan, India