International Journal of Law
ISSN: 2455-2194; Impact Factor: RJIF 5.12
Received: 28-04-2020; Accepted: 12-05-2020; Published: 28-05-2020
www.lawjournals.org
Volume 6; Issue 3; 2020; Page No. 140-145

Rising cyber-crimes threatening Indian web security: A legal analysis

Shibanee Acharya
Student, SOA National Institute of Law, SOA University, Bhubaneswar, Odisha, India

Abstract
Cyber-crime is a type of criminal activity carried out over web. This term is broader in nature as it has twofold effects. The positive aspect is that people are getting aware about the various issues, actively participating and making their views. Besides, the advancements in technology are providing even more opportunities for teenagers. Computers are getting smaller, faster, more powerful and cheaper than ever before. The negative impact arises when people wish to protect their children from the biggest lure of the century. There have been innumerate warnings from the media and law enforcing agencies, yet the problem seems to be escalating. The tragedy is that the people with wrong intentions think it as a safe place for theft. This study examines all the crucial things involved in this subject area. This work aims to analyze the various aspects from the society's point of view. This work does not cover all the corners involved in cyber law but briefly studies some major aspects as per the topic. This work investigates from the societal point of view which shows certain rules in cyber legislations need to be stringent in nature. As a result of which, the ratio of crimes arising in the cyber zone can be controlled for the betterment of people at large. This study also targets the parents to give their time to their children properly, discuss important findings in web, do not be harsh upon them, so that the child might turn rebellious and think twice before telling lie.

Keywords: technology, teenager, children, computer, cyber law, web, crime

1. Introduction
The term 'Internet' is regarded as a connected network of a worldwide system. Millions of servers, computers, printers and routers are connected in each network. It is considered as the super highway of communicating information through networks from state to state or from one country to other. These networks are owned and maintained by various companies, but all the important data and messages are circulated between them without having any regard to the ownership. The reason behind it is the usage of the similar language or protocol to communicate the information. Moreover, Internet security is a larger term which covers the security of the transactions made over the Internet. Generally, it enhances the browser security, authentication & protection of data sent and received via Internet.

However, the term 'crime' takes its adverse effects on all the members of the society at large. Cyber-crime has increased rapidly due to the huge diffusion of the internet services and major digitization of economic activities in order to develop the economies of the country. The huge penetration of the technology lifted the society from lowest level of petty shop-keepers computerizing the billing system to the highest level of state administration and corporate governance. Computers and other electronic devices paved the lives of the humans in a different way. The growth is so deep that humans can not imagine to survive without computers or mobiles.

Cyber-crime is defined as the type of crime which involve a computer and a network. The computer is always used as a weapon to commit a crime in some cases, and it may be the target of the crimes in other cases. Cyber-crimes also indulge various traditional crimes carried out through the web [1]. Traditional crimes includes Internet fraud, hate crimes, credit and account thefts, telemarketing etc. in order to carry out illegal crimes through Internet and computer. The term 'Cyber-crime' involves certain synonyms namely 'high-tech crimes', 'Internet crimes', 'computer crimes' which are used interchangeably when the sources are discussed [2]. The various crimes committed through the Internet includes credit card fraud, child pornography, identity theft etc. Examples of Cyber-crime includes unauthorized access to the personal information of a person without his permission and getting malicious software, viruses, botnets, spyware, Remote Access Trojans illegally.

2. Typology of Cyber-crime
Cyber-crime is recognized as a serious offence as mentioned under the Computer Misuse Act. The Police along with the National Crime Agency take it as a major threat to the society. As a result of which, they will make best possible efforts to eradicate this problem from the society by arresting and prosecuting the offenders. As per the records, the younger generation is getting involved with this crime without knowing about the consequences which may affect their education and future career.

2.1 Hacking
Hacking is regarded as a term which applies to different human activities that interfere with the smooth functioning of computer systems and networks. Due to the ambiguity in this term, most of the legal systems do not operate properly. Various criminal offences which are related to hacking includes computer trespassing to obtain data, damaging a

[1] Grainne Kirwan & Andrew Power, The Psychology of Cybercrime: Concepts and Principles, IGI Global, 2011
[2] Moore, R. "Cyber-crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing, 2005

computer by malware, trafficking in password and other hacking tools, unauthorized access to the computer system and networks etc.

2.2 Malware writing
Malware in terms of service is offered in the underground market. It is designed specifically to gain and control a computer named as Remote Access Trojan [3]. It is an acronym for malicious software which is designed for various functions that includes maintain and gain of a computer without the consent of the operator for collecting the information stored in another system by installing new applications.

2.3 Website defacement
Website defacement is a form of hacking whose end goal is to replace the content of the legitimate website with a different content having a message on religious, political and social significance. It may or may not even depend upon the computer system which runs a particular website or social network.

2.4 Ransomware attack
Ransomware attack is a kind of extortion that is used to encrypt the documents stored on the computer. It is applied in order to deny the access of the legitimate operator in his computer. It is also termed as cryptoware. There exists other type of ransomware that do not encrypt any data and come under the most prolific families i.e blocking the access to the computer otherwise termed as police ransomware. Once the data is extracted from the computer, ransomware demands the victim to initiate the payment procedures and release the important information. This payment is done through an anonymous payment procedure [4].

2.5 Distributed Denial of Service
Distributed denial of service or DDoS attack is termed as a type of crime initiated to make the unavailability of Internet services to the intended users. DDoS is performed using multiple compromised systems that flood the targeted Internet service with bogus requests to exhaust its processing capacity [5]. In one particular instance, DDoS attacks were combined with ransom requests, threating potential victims to make their web site unavailable if they did not make a ransom payment in Bitcoin.

2.6 Computer related fraud
This includes various forms of credit card fraud, money laundering, insider trading, and many other types of white-collar crimes utilizing computers and the Internet as an essential component. The Information Technology Act, 2000 and Indian Penal Code, 1860 provides certain provisions which criminalize all forms of computer related fraud.

2.7 Child Sexual Abuse Material
This includes the production, distribution, exportation, importation, as well as deliberate possession of child abuse materials. The Indian legislation addresses online child pornography in various parts of India. The Information Technology Act, 2000 and Indian Penal Code, 1860 explicitly criminalizes such behaviors as cybercrimes [6].

3. Genesis of legislations
The enormous growth in e-commerce and governance sector of a nation is seen through globalization and computerization during 20th century. Till then, various international transactions and trade were executed through documents which are transmitted through post. Records and evidences were in hard copy format. Though the international trade done through electronic communication, an urgent need was felt for recognizing the usage of electronic records in a proper format. The United Nations Commission on International. In January, 1996 The General Assembly of United Nations had passed a resolution by recommending all other state of United Nation to provide favorable considerations in regard to the Model law in the same manner as that of communicating electronic records.

3.1 The Information Technology Act, 2000
The Information Technology Bill was passed by both the houses of the Indian Parliament in the month of May, 2000. The President gave his assent to the Bill in the month of August which came into force thereafter. It is named as the Information Technology Act, 2000. It includes various cyber laws set up in order to minimize the crime rate. Moreover, it also aims at providing legal framework in accordance to the electronic records carried out through the electronic means. The cyber laws create a major impact on the new economy and e-businesses of the country.

The said Act constitutes various Cyber Regulation Advisory Committee which advice the government regarding the implementation of any rules connected thereto. The Act also recommends to amend certain provisions of Indian Penal Code, 1860, The Indian Evidence Act, 1872, The Reserve Bank of India Act, 1934, The Bankers Books Evidence Act, 1891 whenever it becomes necessary.

India is one of those few countries who enacted various legislations to combat Cyber-crimes. One of such statute is the Information Technology Act, which has included certain terms like tampering of the data, hacking, publishing obscene material in the net etc. These offences are held to be punishable by nature. However, there is lack of international treaties which are unable to track the original sources of crime in various countries. It is also seen that there is a lack of clarity in the implementation of laws and jurisdiction to keep pace with the new forms of Cyber-crimes [7].

3.2 Indian Penal Code, 1860
The most powerful legislation and widely used in the field of criminal jurisprudence is the Indian Penal Code (IPC). This enactment provides the laws and the punishments as per the nature of the crime committed by a person or a

[3] Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, London, UK, 3rd edition, 2011

[4] Alexander Seger, "Cyber Crime and Economic Crime" in M. Edelbacher, P. Kratcoski and M. Theil, eds, Financial Crimes: A Threat to Global Security, 2012

[5] https://www.academia.edu/29564277/White_Paper_Youth_Pathways_into_Cybercrime.October 2016

[6] The Internet Organised Crime Threat Assessment (IOCTA) 2014 https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta

[7] http://www.legalserviceindia.com/legal/article-1019-importance-of-cyber-law-in-india.html

group of persons. It came into force in the year 1860 and amended several times as per the needs of the society. Many special statutes have been came into force having criminal and penal provisions in our country which includes IPC as well. The Information Technology Act, 200 has amended the provisions which dealt with records and documents in IPC by simply inserting the term 'electronic' in order to avoid the confusions.

3.3 The Indian Evidence Act, 1872

This is another legislation which is amended by the Information Technology Act, 2000. Prior to the amendment, all the evidences collected or furnished before the court were in physical form only. When the IT Act provided recognition to all the electronic documents and records, it became necessary that the evidentiary legislations must be amended in the tune of it. The terms like 'digital signature', 'information', 'electronic form', 'secure electronic record' were inserted in the Information Technology Act, 2000 as well as in the Indian Evidence Act, 1872 in order to make these evidentiary in various legislations.

3.4 Advantages of Cyber Legislations

The Information Technology Act, 2000 overrides the outdated laws and operates in a manner to control the rising Cyber-crimes. These legislations will help people to carry out online transactions through credit cards without having any fear of its misuse. The Act functions in such a way that the information provided is not denied in any way through legal framework. It seeks to empower the government departments to accept the filing & retention procedures of the official documents digitally in view of the growth in communications and transactions made through electronic modes. It also proposed for a legal framework for the authentication and origin of the electronic documents and records through digital signature.

On considering e-commerce in India, the Act along with its legislations provide various positive aspects. At first, the implications of these sections for carrying out e-business would be helpful through the usage of email in a valid and legal form to communicate in our country which can be approved and duly produced before the court of law [8]. Various companies will be benefited in carrying out the e-commerce using the legal infrastructure enshrined by the Act. The Act sanctioned and legally validated digital signatures as a result of which it welcomes the corporate companies to issue digital signature certificates. It allows the government to issue various circulars or notifications on the web by heralding e-commerce.

The Act allows the companies to file any form or application with anybody corporate, office, authority which are owned and controlled by the appropriate government by means of any electronic form specified by the appropriate government. It also addresses the important security issues and provides legal definition to the secured digital signatures that would result in passing through security procedures as stipulated by the Government. Under this Act, the corporate sector is vested with statutory remedy if in case anyone tries to breach the computer system or network in order to cause damage and extract important data or information.

[8] https://en.wikipedia.org/wiki/Cybercrime.13th May, 2020

4. Results and Discussion

The rapid growth of the crime against computer system or networks is hatching the attention of the nations. In most of the countries around the globe, existing statutes are not enforceable due to the lack of various aspects affecting it largely. Making people understand about the concept of self-protection is not sufficient to tackle the problem. Countries must enforce stringent legislations and provide all necessary legal protections in an adequate manner. Failing to this will result to the mass destruction in the economy sector. The increasing trend of Cyber-crime ultimately breaching the national borders run with a risk of getting electronic messages blocked by the networks [9]. Only certain countries have amended their statutes as per the need of their society in order to cover half of the crimes and specified punishments according to it. The additional works have been a great deal before the organizations and individuals to feel them secure and confident that attacking the valued systems and information cannot be possible in an easier way.

4.1 Impact on Teenagers

The social networking sites majorly focus on establishing online communication between different individuals or groups in order to share their interest or activities over web. Most of the sites lend their service on online mode and provide the users various methods to communicate or interact with other people through emails or messaging services. It also encouraged distinct ways to share and communicate information [10]. The online websites are operated on a regular basis by millions of users. The features of the sites may differ certainly, but they keep on engaging the users to provide various sorts of information about themselves and continue to offer various types of communication mechanisms that enable them to connect with others.

Mostly, youth or teenagers are the targets of these social sites due to the higher interest of the young people to explore various things over web. They have also acquired these Internet facilities as a regular technology to be used for their benefit. But, the excessive use of these social sites are hampering the future of the youth, as well as they are getting addicted towards these services within a short usage period. Some of them have met with serious psychological problems due to the excessive use of the social networking sites. The personal information of girls and women were leaked and displayed in social networking sites like Orkut and Facebook through multiple accounts created by offenders. This leads to the insecurity of girls and women to aspire for finding friends through these sites.

Orkut was one of the social networking sites which lend free access to own and operate google by its users. This was designed with an aim to provide the users to connect with new friends and maintain the already existent relations. Although it had competitors like Facebook, Myspace etc. but it had frequent users across many countries across the globe. India is one of them. According to a survey, it was seen that Orkut users in India amount to 17.51% of the total

[9] Tripathi A. and Dubey S.,"A study of the need of internet security for consumers at various levels", Journal of Advances in Management Research, 2006, Vol. 3 No.1, pg. 68-74.

[10] International Journal of Internet of Things: Impact of Cyber Crimes on Social Networking Pattern of Girls.2012; 1(1) pg. 9-15

users across the world [11]. Likewise, Facebook also deals with the same problems as that of Orkut.

- Around 48% of youth believes that Internet is the only source to find new friends and develop their friendship. As the social networking sites are catching the interest of the youth majorly, it enables them to get indulged in such a way that youth find it the only process to find new friends. Youth find it more safe and feel confident to communicate and share views with friends irrespective of knowing the consequence of being trapped by the fraudsters. Around 13 million teens across the globe, online communication tools open the door for friendships with other teens near and far.
- While teens are much interested to use social networking sites, their writing skills are becoming different from the original one. They are using shorthand, abbreviations or different slangs while having a chat online. As per the reports of The National Commission, around 85% teens prefer online communication but neglect the proper writing skills or procedure. They must know the basic distinction between the formal and informal writing.
- Cyber bullying also plays a critical role serving negative impact to the youth over online communication. Victims of this crime face any type of rumors and lies spread through these online sites. Bullies misappropriate the pictures of the victims and also harass them through text messages [12]. In some cases, where these bullies are caught and arrested, they tried to commit suicide on their own. As per the survey of The National Crime Prevention Council, most of the teens are indulged in this crime and hamper the interest of other people.
- Another negative impact over youth is sexual solicitation which is growing as a major concern for the society at this point of time. It may take its effect on online sites or chat rooms when an adult tries to indulge himself in an online sexual relationship. A teen may be questioned on various aspects in order to extract his/her personal information, discuss various sexual contents, watch online pornography etc. Around 70% of teens who are solicited on online mode are girls. So, its advisable to all the teens in particular to share their personal photos or talk to know people as per the requirement and try to avoid any talk with the strangers.

4.2 Legislative Provisions

Some of the provisions of the IT Act along with the punishment mentioned are as follows:

- Section 43 deals with 'Damage to Computer system etc.'

Punishment- Compensation for Rupees 1crore.

- Section 66 deals with 'Hacking (with intent or knowledge)'

Punishment- Fine of 2 lakh rupees, and imprisonment for 3 years.

- Section 67 deals with 'Publication of obscene material in e-form'

Punishment- Fine of 1 lakh rupees, and imprisonment of 5years, and double conviction on second offence

- Section 68 deals with 'Not complying with directions of controller'

Punishment- Fine upto 2 lakh and imprisonment of 3 years.

- Section 70 deals with attempting or securing access to computer

Punishment- Imprisonment upto 10 years.

- Section 72 deals with 'For breaking confidentiality of the information of computer'

Punishment- Fine upto 1 lakh and imprisonment upto 2 years

- Section 73 provides with 'Publishing false digital signatures, false in certain particulars'

Punishment- Fine of 1 lakh, or imprisonment of 2 years or both.

- Section 74 deals with 'Publication of Digital Signatures for fraudulent purpose'

Punishment- Imprisonment for the term of 2 years and fine for 1 lakh rupees.

4.3 Trend analysis

As per the statistics available at National Crime Records Bureau, the number of cases registered under Indian Penal Code, 1860 and Information Technology Act, 2000 during 2004-2015 is presented numerically in table 1 and graphically in Figure 1.

Table 1: Number of cases registered during 2004-2015

Year	Indian Penal Code	Information Technology Act
2004	279	68
2005	302	179
2006	311	142
2007	339	217
2008	176	268
2009	276	420
2010	356	966
2011	422	1791
2012	601	2876
2013	1337	4356
2014	2272	7201
2015	3422	8045

***Source*:** National Crime Record Bureau

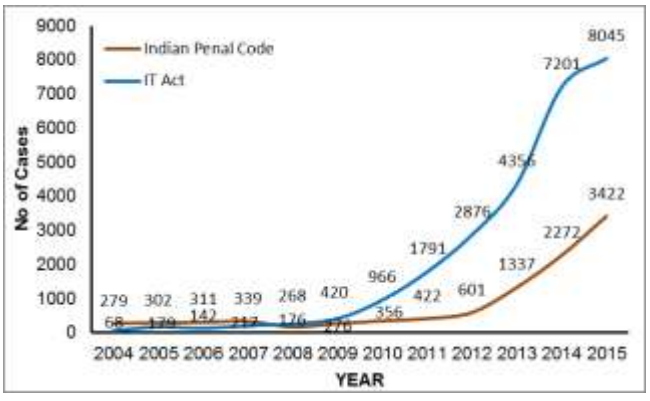

Fig 1: Trend of cases registered during 2004-2015

- During 2004-2009, the total number of cases reported under IPC is 1,683 showing an increase of 503.2%.
- At the same interval, the total number of cases registered under IT Act is 1,294 showing an increase of 1802.9%.
- During 2010-2016, the total number of cases registered under IPC is 8410 showing an increase of 399.7%.

[11] The Hindu Business Line, Google in India's fast lane; Orkut fast rising search query, 2007

[12] https://www.academia.edu/Impact of Cyber-crime issues and challenges/40374418

- At the same interval, the total number of cases registered under IT Act is 25,235 showing an increase of 1850.1%.
- This shows the consistent increase of Cyber-crime cases under IPC and IT Act.
- The dramatic rate of increase of cases under IT Act in both the intervals shows the effective implementation of cyber laws.

5. Recommendations

5.1 Social factors

- The decision-making abilities of the young people must be focused and properly intervened on the concept of hacking. The best way to escalate is to self-challenge by offering pathways towards the achievement in an ethical manner. The potential of the young people can be taken as a positive skill to develop, rather than indulging those in cybercrimes. The requirement of self-esteem and affiliations can divert them from any wrongful activities.
- By educating children in an earlier basis, the danger from the stranger becomes lesser to take effect [13]. The intention of those strangers are identified instantly, as a result of which it becomes impossible for those people to execute their plan on online mode. The awareness programs and campaigns at school level helps the system in a more easier way.
- The Reports of the stakeholders specified that parallel approach should be made in order to make the youth understand the concept of public health approach and their interest. The strategies to prevent the juveniles from committing hacking have focused on the early education and awareness programs conducted in various places. The educational initiative should not only focus on the teachers to train about cybersecurity, but also include the training of cyber skills which are necessary for the youth to participate in extracting advantages of cyberspace.

5.2 Human behaviorism

- In recent years, it is pertinently seen that the rate of Cyber-crime is rising due to the involvement of youth in all the offences enshrined under the IT Act. In order to eradicate the wrong concepts, it is important for the parents to get indulged with their child, spend some time, discuss various aspects, and get aware of the activities that their child performs on online mode. It is the only way to avoid the risk by studying the behavior of the youth.
- Proper monitoring of the child is necessary in order to keep him away from the negative impact of cyberspace. It is the first and foremost duty of the parents to educate their child regarding the usage of web in a proper manner. They must teach the various misconduct and victimization activities committed over web in order to protect their child from those traps. Major problems start to occur when parents take this issue in a negligent way and risk their bond with their child as a result of which it may lead to a generation gap between them.

5.3 Advanced technology effects

- The online environment has always been the hotspot area for the offenders to carry out their plans successfully. But, the fact which can not be neglected is that this online environment has also been the frontier of educating a larger mass within a short span of time. Risk factors also evade away due to the positive aspect of learning the methods to track the hackers [14]. Authorities are trying their best to aware the enlarged society on cybercrime and its ill effects. Some portion of the society are engaging themselves to show their interest in acquiring knowledge on this subject matter.
- Due to the advancement in the technology, various black-marketing activities on online web are being tracked successfully from their original sources. Individuals could take more time to solve this sophisticated system of hacking, but the advanced technology make it possible to stop the large-scale attacks in a short span.

5.4 Proper Law enforcement

- Hacking is becoming the biggest hurdle for the society as well as for the enforcement of various laws. As it is a global issue, it requires several local solutions to be adopted by the police officials while arresting the youth involved in hacking.
- Youth must be provided with enough knowledge regarding cyber security. The stakeholders of cyber security face a lot of challenges due to insufficient capacity to tackle the problem. Solutions must be drawn in order to function properly.
- Youth must be informed about the gravity of offences and directed about the ethical standard of hacking which will be regarded as the initial step to encourage them in a positive way.
- Various precautions and protocols must be maintained in a proper way by the individuals and institutions to minimize Cyber-crime in view of the quantum of increase of cases as envisaged above.
- In order to combat the misconception [15], it is important to inform the youth regarding the online environment specifically stating the consequences of Cyber-crime. They must be made aware about the plan of antisocial individuals while affecting the psychological harm to anyone on online mode.

5.5 Awareness pathways to youth

- All the youth's along with their parents must be informed about the hacking and other cybercrimes prevalent in society by organizing awareness campaigns in schools.
- All the youth's must be given proper education in context of cyber security and the legislations made in India. It can be carried out through online learning modes, adding subjects in school curriculum etc.
- It must be ensured that the awareness programs and campaigns extend to the parents.
- The digital media as well as the traditional media must highlight the dark side of the illegal usage of Internet amongst the youth. They must ensure that all the

[13] Maria Murumaa-Mengel, "Drawing the Threat A Study on Perceptions of the Online Pervert among Estonian High School Students", 2015, 23(1), pg. 1-18.

[14] Moon *et al*.., A general theory of crime and computer crime, 2007, pg. 772

[15] Europol, The Internet Organised Crime Threat Assessment (IOCTA), The Hague, 2014

parents, educators and children must be supplied with online resources
- Vulnerable youth working with different Practitioners must extract proper training of understanding the behavior of hacking and must be supplied with necessary support things.

6. Conclusion

Thus, it can be clarified that cybercrime may cause harm to a person, to the security of a nation and to the financial health as well. The various high-profile issues have become the subject of discussion which may include crimes like copyright infringement, child pornography, hacking, digital forgery, unwarranted mass-surveillance. These are also considered to be a major aspect to look after, as it largely affects the privacy by hesitantly disclosing the confidential information illegally. By summing up the topic, it can be stated that in order to minimize the rate of crime in web, stringent legislations need to be enforced and implemented in a proper manner. As the society is becoming more dependent on the technological advancements, the fraudsters are targeting to commit crime more comfortably through web. The law makers have to put extra efforts to keep the crime rate as minimum as possible. Technology is functioning like a double-edged sword having both positive and negative impact. Hence, it should be foreseen by the law makers and rulers to ensure the increasing growth of the technology in a healthy way and restrict people to misuse it by committing different crimes over web.

7. References

1. Alexander Seger, “Cyber-crime and Economic Crime” in M. Edelbacher, P. Kratcoski and M. Theil, eds, Financial Crimes: A Threat to Global Security, 2012.
2. Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, London, UK, 3rd edition, 2011.
3. Europol, The Internet Organised Crime Threat Assessment (IOCTA), The Hague, 2014.
4. Grainne Kirwan & Andrew Power, The Psychology of Cybercrime: Concepts and Principles, IGI Global, 2011.
5. https://www.academia.edu/29564277/White_Paper_Youth_Pathways_into_Cybercrime.October 2016
6. https://www.academia.edu/40374418/Impact of Cyber-crime issues and challenges. October 2013
7. http://www.legalserviceindia.com/legal/article-1019-importance-of-cyber-law-in-india.html
8. https://en.wikipedia.org/wiki/Cybercrime.13th May, 2020.
9. International Journal of Internet of Things: Impact of Cyber-crimes on Social Networking Pattern of Girls 2012; 1(1):9-15.
10. Maria Murumaa-Mengel, “Drawing the Threat A Study on Perceptions of the Online Pervert among Estonian High School Students”. 2015; 23(1):1-18.
11. Moon *et al*., A general theory of crime and computer crime, 2007, pg. 772
12. Moore R. "Cyber-crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing, 2005.
13. The Internet Organised Crime Threat Assessment (IOCTA), 2014. https://www.europol.europa.eu/content/internet
14. organised-crime-threat-assesment iocta.29th September, 2016.
15. The Hindu Business Line, Google in India’s fast lane; Orkut fast rising search query, 2007.
16. Tripathi A. and Dubey S.,"A study of the need of internet security for consumers at various levels", Journal of Advances in Management Research. 2006; 3(1):68-74.