ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Study of Cyber Crime & Their Ethics in India

Shreyas Dingankar

Assistant Professor, Institute of Management and Entrepreneurship Development, Pune, Maharashtra, India

ABSTRACT: In this paper we have discussed the different ethics in the cyber crime. The ethics centers and program devoted to business ethics, legal ethics, bioethics, medical ethics, engineering ethics, and computer ethics have sprung up. These centers are designed to examine the implications of moral principles and practices in all spheres of human activity on our lives. Cyber crime is emerging as a serious threat. World Wide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel. This article is an attempt to provide a glimpse on cyber crime in India. This article is based on various reports from news media and news portal.

KEYWORDS: Cyber crime, Ethics, Hacking, Phishing, Vishing.

I. INTRODUCTION

Ethics can be viewed from two angles, normative and prescriptive. First, ethics refers to well-based standards of right and wrong that prescribe what humans ought to do, usually in terms of rights, obligations, benefits to society, fairness, and specific virtues. Ethics, for example, refers to those standards that impose the reasonable obligations to refrain from rape, stealing, murder, assault, slander, and fraud. Ethical standards also include those that enjoin virtues of honesty, compassion, and loyalty. And, ethical standards include standards relating to rights, such as the right to life, the right to freedom from injury, the right to choose, the right to privacy, and right to freedom of speech and expression. Such standards are adequate standards of ethics because they are supported by consistent and well-founded reasons.

Secondly, ethics refers to the study and development of personal ethical standards, as well as community ethics, in terms of behavior, feelings, laws, and social habits and norms which can deviate from more universal ethical standards. So it is necessary to constantly examine one's standards to ensure that they are reasonable and well founded. Ethics also means, then, the continuous effort of studying of our own moral beliefs and conduct, and striving to ensure that we, and our community and the institutions we help to shape, live up to standards that are reasonable and solidly-based for the progress of human beings Definition "Ethics are moral standards that help guide behavior, actions, and choices." Ethics are grounded in the notion of responsibility (as free moral agents, individuals, organizations, and societies are responsible for the actions that they take) and accountability (individuals, organizations, and society should be held accountable to others for the consequences of their actions).

In most societies, a system of laws codifies the most significant ethical standards and provides a mechanism for holding people, organizations, and even governments accountable. The world of Internet today has become a parallel form of life and living. Public are now capable of doing things which were not imaginable few years ago. The Internet is fast becoming a way of life for millions of people and also a way of living because of growing dependence and reliance of the mankind on these machines. Internet has enabled the use of website communication, email and a lot of anytime anywhere IT solutions for the betterment of human kind. Internet, though offers great benefit to society, also present opportunities for crime using new and highly sophisticated technology tools. Today e-mail and websites have become the preferred means of communication. Organizations provide Internet access to their staff. By their very nature, they facilitate almost instant exchange and dissemination of data, images and variety of material.

This includes not only educational and informative material but also information that might be undesirable or anti-social. Regular stories featured in the media on computer crime include topics covering hacking to viruses, web-jackers, to internet

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

pedophiles, sometimes accurately portraying events, sometimes misconceiving the role of technology in such activities. Increase in cyber crime rate has been documented in the news media.
Both the increase in the incidence of criminal activity and the 2 possible emergences of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement.

II. CYBER SPACE-CYBER CRIME

Cyber space is a collective noun for the diverse range of environments that have arisen using the Internet and the various services. The expression crime is defined as an act, which subjects the doer to legal punishment or any offence against morality, social order or any unjust or shameful act. The "offence" is defined in the Code of Criminal Procedure to mean as an act or omission made punishable by any law for the time being in force. Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. III. TRADITIONAL CRIME – CYBER CRIME Computer crime mainly consists of unauthorized access to computer systems data alteration, data destruction, theft of intellectual properly. Cyber crime in the context of national security may involve activism, traditional espionage, or information warfare and related activities. Cyber crimes have been reported across the world.
Cyber crime is now amongst the most important revenue sectors for global organized crime. Because of this, the potential risks associated with malware have risen dramatically. Unlike in traditional crimes, the Information Technology infrastructure is not only used to commit the crime but very often is itself the target of the crime. Pornography, threatening email, assuming someone's identity, sexual harassment, defamation, SPAM and Phishing are some examples where computers are used to commit crime, whereas viruses, worms and industrial espionage, software piracy and hacking are examples where computers become target of crime.
There are two sides to cyber crime. One is the generation side and the other is the victimization side. Ultimately they have to be reconciled in that; the number of cyber crimes committed should be related to the number of victimizations experienced. Of course there will not be a one-tone correspondence since one crime may, inflict multiple victimizations multiple crimes may be responsible for a single victimization. Some crimes may not result in any victimization, or at least in any measurable or identifiable victimization. The obvious effect of cyber crime on business is the evolving threat landscape. 'The motive of the attacks has changed over time. Earlier, the intent of the attacker was to gain fame although the motivation was criminal. Cyber crime economics are too compelling to subside.

III. CYBER SPACE-CYBER CRIM

Cyber space is a collective noun for the diverse range of environments that have arisen using the Internet and the various services. The expression crime is defined as an act, which subjects the doer to legal punishment or any offence against morality, social order or any unjust or shameful act. The "offence" is defined in the Code of Criminal Procedure to mean as an act or omission made punishable by any law for the time being in force. Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity

IV. CYBER CRIME VARIANTS

There are a good number of cyber crime variants. A few varieties are discussed for the purpose of completion. This article is not intended to expose all the variants. The readers are directed to other resources.

4.1 Cyber stalking

Cyber stalking is use of the Internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. Stalking generally involves harassing or threatening behavior that an individual

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property.

4.2 Hacking

"Hacking" is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. Hacking had witnessed a 37 per cent increase this year.

4.3 Phishing

Phishing is just one of the many frauds on the Internet, trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account for some reason. Customers are directed to a fraudulent replica of the original institution's website when they click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred. The fraudster then has access to the customer's online bank account and to the funds contained in that account. F-Secure Corporation's summary of 'data security' threats during the first half of 2007 has revealed that the study found the banking industry as soft target for phishing scams in India

4.4 Cross Site Scripting

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls.

4.5 Vishing

Vishing is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private .personal and financial Information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company, and associated with a bill-payer. The victim is often unaware that VoIP allows for caller ID spoofing, inexpensive, complex automated systems and anonymity for the bill payer. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals.

4.6 Cyber Squatting

Cyber squatting is the act of registering a famous domain name and then selling it for a fortune. This is an issue that has not been tackled in IT act 2000.

4.7 Boot Networks

A cyber crime called 'Boot Networks', wherein spamsters and other perpetrators of cyber crimes remotely take control of computers without the users realizing it, is increasing at an alarming rate. Computers get linked to Boot Networks when users unknowingly download malicious codes such as Trojan horse sent as e-mail attachments. Such affected computers, known as zombies, can work together whenever the malicious code within them get activated, and those who are behind the Boot Networks attacks get the computing powers of thousands of systems at their disposal. Attackers often coordinate large groups of Boot-controlled systems, or Boot networks, to scan for vulnerable systems and use them to increase the speed and breadth of their attacks. Trojan horse provides a backdoor to the computers acquired. A 'backdoor" is a method of bypassing normal authentication, or of securing remote access to a computer, while attempting to remain hidden from casual inspection. The backdoor may take the form of an installed program, or could be a modification to a legitimate program. Boot networks create unique problems for organizations because they can be remotely upgraded with new exploits very quickly and this could help attackers pre-empt security efforts.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

V. VULNERABILITY

The Open-Source Vulnerability Database (OSVDB) project maintains a master list of computer - security vulnerabilities, freely available for use by security professionals and projects around the world. Vulnerability information is critical for the protection of information systems everywhere: in enterprises and other organizations, on private networks and intranets, and on the public Internet.

VI. INDIAN CRIME SCEN

The major cyber crimes reported, in India, are denial of services, defacement of websites, SPAM, computer virus and worms, pornography, cyber squatting, cyber stalking and phishing. Given the fact that nearly $ 120 million worth of mobiles are being lost or stolen in the country every year, the users have to protect information, contact details and telephone numbers as these could be misused. Nearly 69 per cent of information theft is carried out by current and ex-employees and 31 per cent by hackers. India has to go a long way in protecting the vital information. Symantec shares the numbers from its first systematic survey carried out on the Indian Net Security scene: The country has the highest ratio in the world (76 per cent) of outgoing spam or junk mail, to legitimate email traffic. India's home PC owners are the most targeted sector of its 37.7 million Internet users: Over 86 per cent of all attacks, mostly via 'bots' were aimed at lay surfers with Mumbai and Delhi emerging as the top two cities for such vulnerability.

VII. CONCLUSION

Threats of cyber crime is left unchecked will be disastrous on the nation, society, economy and security. It is the collective responsibility of all to ensure that technology is not abused. Be a disciplined user.

REFERENCES

[1] CYBER CRIME TODAY & TOMORROW, THIRU DAYANITHI MARAN, HTTP://W W W. D. M ARAN.NIC.IN/SPEECHDISPLAY.PH,P?JD=I?9, 2008.
[2] POLICE MAKE HEADWAY, THE HINDU, SUNDAY OCTOBER 29 2006.
[3] CYBER CRIMES ON THE RISE IN STATE - KERALA: THE HINDU MONDAY OCT 30 2006.
. [4] NOW A PUNE BASE FOR NET'S CYBER COPS THE HINDU SUNDAY NOV 26 2006.
[5] BANK CUSTOMERS FACE PHISHING, THE HINDU, COIMBATORE, MONDAY AUGUST 20 2007,
[6] PHISHING ATTACKS AGAINST INDIANS: F-SECURE, THE BUSINESS LINE MONDAY JULY 232007. [7]TAMIL NADU TO COME OUT WITH ^ IT SECURITY POLICY SOON, THE HINDU, SATURDAY, OCT 27, 2007. [8]YOUTH IN JAIL FOR SENDING EMAIL THREAT THE HINDU FRIDAY AUG 10, 2007.
[9] PHISHING FOR TROUBLE: THE HINDU WEDNESDAY, JAN 17, 2007.
[10]CYBER CRIME UP POLICE FOUND WANTING, CHANDIGARH TRIBUNE MONDAY MAY 28, 2001. [11]NASIK POLICE PLAY BIG BOSS FOR INTERNET VOYEURS, HINDUSTAN TIMES, SUNDAY, OCT 28 2007. [12] LOSSES DUE TO CYBER CRIME CAN BE AS HIGH AS $40 BILLION, THE HINDU BUSINESS LINE DATE MAY 21 2007 DOWNLOADED 20 OCT2007.
[13] KOLKATA MAN THREATENS TO BLOW UP STOCK EXCHANGES ARRESTED. EXPRESS INDIA.COM SUN 28 OCT 2007.
[14] SUHAS SHETTY CYBER CRIME CASE, FIRST CONVICTION IN INDIA UNDER ITA-2000. HTTP:/ 7 W W W. N A A V I. O R G /C L _ E D I T O R I A L _ 0 4 /SUHAS_KATTI_CASE.HTM
[15] WEB PORTAL CALL CENTER TO TACKLE CYBER CRIME, THE HINDU BUSINESS LINE, TUESDAY, JUL 31, 2007
[16] SHREYAS DINGANKAR Www.Ijmr.Net.In INTERNATIONAL *Journal In IT And Engineering, Vol.03 Issue-10, (October, 2015)*

BIOGRAPHY

Shreyas Upendra Dingankar is Assistant Professor in Institute of Management and Entreprenurship Development College, Pune Bharati Vidyapeeth University Pune. He has done his MBA from Pumba Pune University in 2011 and His Research Interest is in Cyber Crime.