International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Cyber Crime: Critical View

Rita Dewanjee[1], Dr. R. Vyas[2]

[1]School of Information Technology, MATS University, Raipur, C.G., India – 493447,

[2]IIIT Allahabad, UP, India – 493447,

Abstract: ***The contribution of this research paper is an overview on cyber crime and the ethical issues related to this field. Centre of focus are the issues connected to the massive increase in cyber crime ratio. Since last few years several billions of dollars per year are exhausted for combating cyber crime issues efficiently. The factors affecting the cybercrime have different laws of treatment in different countries that often overlook aspects of the problem and investigation in the depth of the issues with different methods, are playing key role . Not only the method of fighting against the cyber crime but also the juridical issues and technical challenges involved in fighting cybercrime may not be understood. Ethical aspects are often set aside – as shown by the various battles government have taken recently to address the cybercrime issues. This paper, reviewed on different backgrounds, will through light on those aspects, and attempts to answer the several raised questions subsequently.***

Keywords: Cyber Crime, Ethical Issues, Cyber Attacks, Cyber Security, Cybercrime

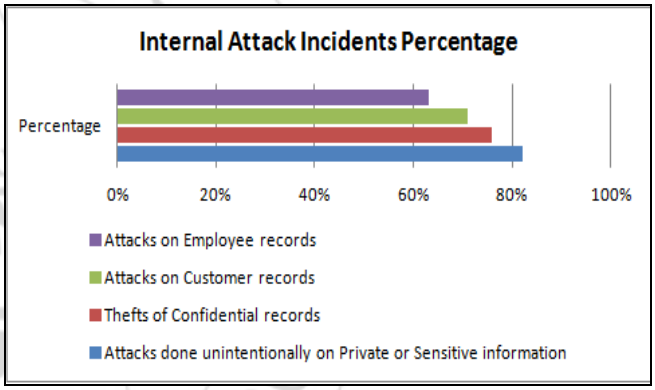
1. Introduction

Crime is a term which gives a scenario and impression of an illegal activity and when it is merged with Computer or Cyber creates more wide and pan global issues. It is a term used mostly to describe criminal activity in which computers or computer networks are a tool, a target or a place of criminal activity.

We may differentiate between Cyber Crime and Computer Crime because cybercrime is basically associated with the use of internet and network, whereas the computer crime may or may not involve networks. [1]. Cybercrime is the crime covering all

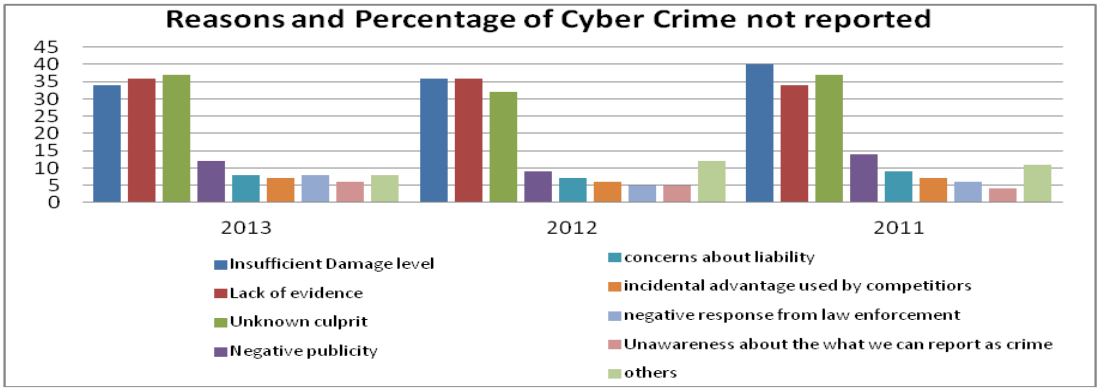
forms of crimes done with the help of computer networks. The target may be itself a Computer or others. Most of the Cybercrime issues are related with the problems like security of financial dealings, prohibiting maltreatment of credit card information, providing security for information during online transactions, preserving privacy and confidentiality of e-mails and the attack on privacy. The one more major issue which is continuously increasing is the matter of specific companies who are handling billing for the adult website industry. Those companies are progressively more the targets of cyber crooks looking to access credit card details and attack on cash [4].

The survey done in 2014 by US state of Cyber Crime and based on the report [2] the ratio of insider attack and the outsider attack is shown below -



Horrific intentions of cyber criminals are a big concern for the society nowadays. Across the globe all countries, Governments are moving and taking plans across the globe to tackle the expanding wave of cyber crimes.

In organization, cybercrime may be categorized in inside and outside attacks. Most of the time when inside attack is made no legal action took place because the survey report of 2014 of CERN says that following reasons were not referred for legal action as shown below –



Reasons and Percentage of Cyber Crime[2]

2. The Types of Cyber Crime

Whenever any crime is committed over the internet it is called Cyber crime. As per the recent reports that were available at emc.com in 2014, 11% per year increase ratio is found and nearly 500,000 cyber attacks recorded in RSA Anti Fraud Command Center. [20]

The Cyber crime is taking a form of "As A Service" and market related to this is tremendously growing in recent years. As per the research of RSA the 4,00,000 malware variants are developed every week.[7].
As per my research all cyber crimes may broadly be categorized in -

- Crimes related to Telecommunication
- Crimes based on personal issues

Crimes Related to Telecommunication

Communication crimes of this category basically effect the large group of peoples. When an organization is mostly depends on Digital Information System and using that for the activities which are illegal in aspects of law come under the Telecommunication Cyber Crime. Cyber Criminals are using different front end services to hide their actual profession. The other most common example of telecommunication theft is access of PBX to obtain the services of dial in/dial out through individual or by the group of peoples.

People use others telecommunication services illegally and without the knowledge of the owner. The third category of telecommunication crime is piracy of digital content. When we publish any ones personal objectionable data without bringing that in their knowledge comes in this category of telecommunication theft. Apart from this, financial thefts by individual or by the group of peoples like for Tax Evasion, Money Laundering, Extortion, terrorism, investment frauds, malicious fund transfers etc are the example of these category of Cyber Crimes.

Crimes based on Personal Issue

Sometimes reasons of cybercrime are unintentional and by mistake. People unknowingly just for fun may send an email or make unauthorized access to another user 's space. They may do not have any intention to commit crime but for fun or for fake repo may indulge in with such activities. Another example is like sometimes only for self ego satisfaction a company person after unjustified firing from his job may harm company data or may disseminate the confidential information so that the opponent party can breach the security system.

A Person may Steal the identity of his higher authority and can steal the confidential data for black money. A psychologically sick person may disseminate malicious software or viruses to harm other people being sick from progress of his/er colleagues. Social media Chat rooms may be another common place of cyber crime where children are mostly found soliciting and Abused . The FBI keep watching frequently the Chat rooms to stop this.

3. Ethical Challenges: Analytical View

Cyber crime ethics may be taken as a science of study where we deal with what should be the actual course of reaction of a person for an activity. ACM suggested 10 ethical standards to deal with a situation and avoid the crime. The standards basically focus on not to harm, damage, interfere, steal or breach information or resources without owner's permission and knowledge and to respect other's privacy.[8]

The cyber crime has social problems like virus, hacking, work place privacy rights and adverse impact of internet contents on kids. The social cyber crimes may be tracked by latest technologies like VPN, IDS, Protocols, Passwords, Encrypting methods, Firewalls etc. but solution suggested are studied more by the hackers to find out the loophole and crack it. These questions enforced ethical principles to be applied.[13,14]

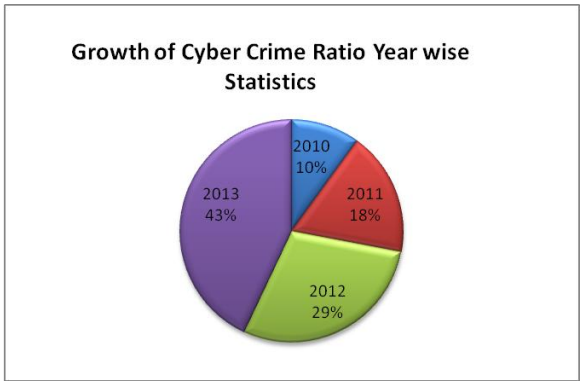
Cyber Crime is a global problem. To fight with the issue everyone must be educated not only the victim, protester, law professionals, IT professionals and specially the Cyber community. Legislation in few countries started long back from 1970 from USA with various acts to prevent cyber crime and forced attackers to think twice before attempting any attack to any system or individual. The various legislation acts are -

1970	Freedom of Information Act
1980	Privacy Protection Act
1987	Computer Security Act
1997	Consumer Internet Privacy Protection Act
1997	Data Privacy Act
1998	MITI Legislation for Ecommerce
1999	Information Technology Act
2000	NSW Electronic Transactions Act
2000	Data Protection Act
2000	Electronic Transactions Regulations

4. Case Study

The popularity of increasing internet and interest in computer offense, morals and privacy has gained momentum. For example, in July, 2001, MSNBC.com reporter Bob Sullivan reported that the personal data was posted up in a chat room. [5]

In India legislative act implemented as IT act 2000. In recent research paper of May 2015, the growth ratio of cyber crime is shown 51.5% . The graph below shows the cybercrime ratio from 2010 to 2013 in India [16]



The MD and Head of thematic investing at Bank of America Merrill Lynch, Mr. Sarbjit Nahal stated more than 80 to 90 million cyber security events happened per year where approx 400/minute new threats and up to 70 percent of attacks were undetected". [17]

From FORBS.com, Steve Morgan, 2015 stated cyber insurance market – mainly a U.S. market – has grown from $1 billion to $2.5 billion over the past two years, and it is expected to grow dramatically and expand globally over the next five years.[18]

The Mcafee.com says Cyber crime is a growing industry. This industry includes more profits and less risk. The global economy from cybercrime is of more than $400 billion.[19] The crime may be in form of online fraud, theft or terrorism. Various organizations like IBM X-Force, ISSA, HP, Symantec, Norton , Fireeye, SANS, OWASP, FIRST, ISF, IAPP, ISACA, AEHIS, IIA, CIUSPA, CSA, ISFS, EWF, CERT, CFO and many more organizations working 24*7 to monitor the latest threats and digital attacks.[20]

5. Conclusion

As the Cyber Crime is growing in wide scale and becoming a global issue. Regardless of regional and national boundaries researchers are working together to find out all possible solutions. Various legislative acts are enforced and implement. Organizations are instructed to abide and follow the safety measures. To fight with Cyber Crime, Cross-Domain Solutions are becoming popular to resolve issues.

Cross Domain Solutions suggest both the parties to follow protocols and standards. The parties using such solutions are communicating across the system's hardware and software for authentication and data transfer. Cross domain solutions provide seamless sharing and access of information. Other Safety measures like checking the person in ethical behavior on moral basis before employment or assigning such confidential work must be done.

The Educational Institutes can play vital role to make a strong ethical base by including such subjects as compulsory ones. Government may do frequent checking on Cyber Community for illegal services and face them to strictly follow the standards. The professionals also be motivated to be honest with their job roles and their services shall be recognized time to time, so that to encourage them to abide by morals and not to move away from ethical culture.

References

[1] Information-retrieval.info/cybercrime/index.html
[2] Source: 2014 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, April 2014
[3] http://www.dbr.shtr.org/v_3n1/dbrv3n1c.pdf
[4] Asthana, R.G.S. (2001) "E terrorism threatens E business", June 1-15, Vol. 5, No. 15, Computer World
[5] http://www.profhelp.com /crime/computercrime .pdf
[6] http://threatchaos.com/2009/03/stay-calm-people cyber-crime-does-not-reap-1-trillion-in-profits
[7] https://www.emc.com/collateral/white-paper/rsa- white-paper-cybercrime-trends-2015.pdf
[8] http://scecsal.viel.co.ke /images/f/fe/Computer_ And _Internet_Crimes-_Ethical_Issues.pdf
[9] http://cabrillo.edu /~shodges/cs1/notes/ cis1. chapter15.pdf
[10] https: //cps182cybercrime. wordpress.com/ethical-issues/
[11] http:// mercury.webster.edu /aleshunas /COSC% 205130 /Chapter-23.pdf
[12] http://www.apu.ac.jp/~gunarto/it1.pdf
[13] " ETHICAL ISSUES IN CYBERAGE ", Rajeev Kumra, R.K. Mittal, Delhi Business Review ? Vol. 3, No. 1, January - June 2002
[14] http://www.aitp.org/news/93013/How-Ethical-Theories-Apply-to-IT-Professionals.htm
[15] http:// www.aitp.org/news/95365/Ethical- Decision - Making-and-the-IT-Professional.htm
[16] "Shaji. N. Raj ",ISSN (Online): 2347-1697 International Journal of Informative & Futuristic Research (IJIFR) Volume - 2, Issue - 9, May 2015 21st Edition, Page No: 3120- 3128
[17] http:// www.welivesecurity.com /2015/09 /09/cybercrime-growing-concern-americans, " The sad stats on state of cyber security: 70% attack go unchecked , BY KARL HOMAS POSTED 9 EP 015 - 01:24PM
[18] http://www.forbes. com/sites/stevemorgan /2015/10/16/the-business-of-cybersecurity-2015-market-size- cyber-crime-employment-and-industry-statistics, OCT 16, 2015 @ 08:40 AM
[19] http://www.mcafee.com/in/resources/reports/ rp-economic-impact-cybercrime2.pdf
[20] http://cybersecurityventures.com/cybersecurity-associations
[21] https:// www.emc.com/ collateral/ white-paper / rsa-white-paper-cybercrime-trends-2015 .pdf