RESEARCH REVIEW JOURNALS
Volume-04
Issue-05
May-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

A Study on Data Privacy, Security of Cyber Crime

[1]Pelasur Chandrakumar Swamy and [2]Dr. Gireesh Kumar J

[1]Research Scholar, Himalayan University, Faculty of Law, Itanagar, AP
[2]Research Supervisor, Department of Sociology, Himalayan University, Itanagar, AP

ARTICLE DETAILS

Article History
Published Online: 15 May 2019

Keywords
Data Privacy, Security, Cyber Crime, information, cyberspace.

ABSTRACT

This study discusses the issues of cybercrime and what is being done to prevent it. Cyber criminals take advantages of vulnerabilities by using viruses, bots, etc to cause damage and/or maybe steal information. There are ways that this can be minimized by being aware of what the problems are. There are many problems but common ones are discussed. Not can these problems be solved on an individual or organization level but also on a global level. This study will look at what cybercrime is and three topics that discuss the problems with cybercrime and how to prevent it.The information age has made the public and private sectors of modern society increasingly dependent on technology, in which telecommunications play a vital role. Over the past thirty years, developed nations' transit from the industrial era to the new information age has enabled them to develop the nascent technology and produce ever greater quality in standards and value. The past decades have also delivered many opportunities in which the flaws and faults of the system have been exploited and mended, by hackers and legitimate users alike. The new society has engendered new types of crimes, such as phishing and botnets, and facilitated the commission of old crimes, for example the violation of intellectual property rights, with new technology facilitating breaches of copyright in music, films and software. As society grows ever more reliant on these technologies, so does the concern for security, especially in cyberspace. The emancipation of the internet has leaped ahead of the judicial system, but the authorities have taken heed and the wheels of the legal machine have started turning. The difficulty, however, has been that the internet-based society has no physical boundaries and thus much traffic escapes national supremacy.

1. Introduction

In present day world we utilize computer systems for everything; searching the world wide web, online shopping, accessing bank accounts, Email, as well as internet gaming as some examples. Communication is actually quicker plus more reliable than in the past that has permitted more to be achieved in a certain day. The issue is the same as anything else; vulnerability. You will find people that hack into computers and also the networks of companies as well as government agencies. The issue is the fact that very sensitive details could be stolen and/or eliminated. There must be a lot more focus on the security of computer systems as well as the web.The globalization of economic, political and social activities, supported by an increasing use of the Internet and other information and communication technologies, raises a wide range of questions regarding privacy and the protection of personal data. This includes questions related to data protection principles, such as those established by the European Union and the Council of Europe (e.g. ETS 108 and Rec R(87)15 on the use of personal data in the police sector), and the investigation of cybercrime, but also questions related to data retention, the increasing trend towards authentication of ICT users, the relationship between service providers and law enforcement and others. Countries developing cybercrime legislation therefore need to be familiar with relevant privacy and data protection issues.

Cybercrime as well as cyber security are actually attracting increasing interest, both for the relevance of Critical Information Infrastructure to the national economy as well as security, as well as the interplay of the policies tackling them with ICT sensitive' liberties, like information and privacy security. This particular analysis deals with the topic in 2 ways. On the one hand, it is designed to cast light on the (legal substantive) nature of, and relationship between, cyber and cybercrime security, which are presently terms of hype' (and consequently it's descriptive). On the other hand, it explores the chance of reconciling information protection as well as privacy with the protection against cybercrime and also the goal of a cyber-security policy (and consequently it explores causation). As a result, the subject falls in the security vs. privacy' wishes and debate particularly to take a look at if it's feasible to create rights that are human by design' security policies, i.e. a security policy that reconciles both security as well as human rights. The argument hinges of mine depends on a clarification of the phrase cybercrime' (and cyber security), both by creating on the literature? Which recognises the mix of standard crimes committed by electronic means (broad cybercrime or maybe off line crimes), and novel crimes possible just in the internet atmosphere (narrow cybercrime or maybe on the internet crimes)?and on authentic interpretations in terms of the connection between cybercrime as well as cyber security is involved.We see an increasing adaptation of "conventional" crime to cybercrime because of the digitalization, convergence of technologies and globalization of ICT. Traditional measures on investigations do not meet the demands of these changes; therefore special procedures need to be developed.

The question is, what measures can be taken by governmental and police authorities to adapt to and restrain

this development in a way that existing privacy rights are preserved? To what extent are authorities free to use personal data and from what sources? There is publicly available data from the Internet and other public sources, but also data acquired in the execution of public tasks, often available in governmental databases. Are criminal investigators allowed to use the data in the same way other governmental authorities use these sources?

Because of the international nature of crimes, international coordinated investigations and the use of personal data must be made possible, but with a sharp eye on their limitations in the interest of human rights and specifically the protection of the privacy of individuals and taking into account the evolution of data availability. The key questions to confront are: how can the tension between privacy protection and criminal investigation be regulated at acceptable levels? And; what adaptations to the existing regulatory framework are needed? In a study by Privacy International3 many European states are not considered capable of upholding human rights standards on privacy. Only Greece is considered to have significant protection and safeguards. Maybe the present study can improve our "score". The purpose of this study is be to give insight and guidance to countries as to how to make cybercrime investigations compatible with data protection and privacy concerns, in particular when implementing the procedural provisions of the Convention on Cybercrime.

Certainly when an investigation into trans-border dataflow is required, it is essential to have sufficient guarantees that authorities are not bypassing fundamental rights. In the comments to the European Convention on Human Rights, it is recognized that essentially, it should make no difference for data users or data subjects whether data processing operations take place in one or in several countries. The same fundamental rules should apply and data subjects should be given the same safeguards for the protection of their rights and interests.Although these rules apply, we must also ensure that they will not be bypassed in practice by investigative authorities and that deviations will only be possible in exceptional cases. In general this is an accepted principle of national and international laws, but in practice guarantees and policies in this respect is not very visible. European legal authorities should bear this in mind when exercising their authorities. In today's world we use computers for everything; searching the internet, online shopping, accessing bank accounts, Email, and online gaming as some examples. Communication is faster and more reliable than in the past which has allowed more to be accomplished in a given day.

Table 1.1: Constraints/ characteristics in Cyber crime

1	Low marginal cost of online activity due to global reach	6	concrete regulatory measure
2	Lower risk of getting caught	7	Lack of reporting and standards
3	Catching by law and enforcement agency is less effective and more expensive	8	Difficulty in identification
4	New opportunity to do legal acts using technical architecture	9	Limited media coverage
5	Official investigation and criminal prosecution is rare; not very effective sentences	10	cyber crimes are done collectively and not by individual persons

Table: 1.2: Different areas of cybercrimes

Financial	Using fake websites to market products so as to get the credit numbers
Cyber	Spreading child pornography or sexually implicit material
pornography	
Marketing strategies	Selling narcotics or weapons online
Intellectual Property	Software piracy, copyright infringement, trademark violations, ±eft of computer code
E-Murder	Manipulating medical records

Political	Abuse of public fords by altering data, bribery" by altering data
Information piracy and forgery	Perfect reproduction of original documents such as social security cards, birth certificates, etc...
Money laundering and evasion	Bypassing die banking system and taxation authorities by concealing the orisin of ill-Eotten money
Electronic terrorism	Electronic intruding into government websites to bring them down
Eject xonic funds	Financial mstirjtians use electronic fund transfer systems and
transfer fraud	hackers intercept them and divert the funds
E-mail logic bombs	Event date programs that do something when a certain went occurs
Internet time thefts	Stealing user name and password from user to use their account time
Hate commercial	Building a website to promote hate or racial hate
Altering websites	deleting web pages, uploading new pages: controlling messages conveyed by the website
Computer viruses	using malicious code or software to cause destruction to information

The problem is just like anything else; vulnerability. There are individuals that hack into computers as well as the networks of businesses and government agencies. The problem is that sensitive data can be stolen and/or destroyed. There needs to be more focus on the security of computers and the internet. This study will focus on the lack of efforts to prevent cybercrime as well as problems associated with it, how cyber security can be improved, and what has been done in response to cybercrime.The world has gotten further developed in correspondence, particularly after the innovation of the internet. A main point of interest confronting the present society is the expansion in cybercrime or e-crimes (electronic crimes), another term for cybercrime. Consequently, e-crimes present dangers to countries, associations, and people over the globe. It has gotten far and wide in numerous pieces of the world, and a large number of individuals are survivors of e-crimes. Given the genuine idea of e-crimes, its worldwide nature, and suggestions, plainly there is an essential requirement for a typical comprehension of such crime internationally to manage it adequately. This part covers the definitions, types, and interruptions of e-crimes. It has additionally centered on the laws against e-crimes in various nations. Cyber security and looking through strategies to get made sure about are additionally important for the examination.

These are a lot of different areas of computer crimes which means there are many opportunities for a hacker to be successful. How they perform these crimes is another important issue. Knowing what they use will give us a better way to help minimize these crimes. “Unauthorized Access is the main tool used by Criminals. Unauthorized access means any kind of access without the permission of rightful owner or in charge of the computer, computer system or computer network.”

2. Review of literature

Harjinder Singh Lallie, et al (2020) - The COVID 19 pandemic became a remarkable unprecedented event which changed the lives of vast amounts of citizens globally resulting in what became typically called the new normal in phrases of societal norms as well as the manner in which we live and work. Apart from the remarkable effect on business and society like an entire, the pandemic generated a set of special cybercrimes connected conditions that also affected society and business. The increased anxiety brought on by the pandemic heightened the likelihood of cyber-attacks succeeding corresponding with a growth in the amount as well as assortment of cyber-attacks.

Vinayak Pujari (2020) -As it is understanding that this's the era in which maximum of the points are thru typically on the internet beginning from internet major business to the internet offer. Meanwhile the internet is viewed as common stage, anyone is able to use the assets of the web at anyplace. The web technology has been by means of by the exceptional individuals for criminal occasions including unlawful access to other's network, swindles etc. These unlawful crimes or even the offense relevant to the web is actually named as cybercrime. To be able in order to break and / or to penalize the cyber criminals the phrase named as Cyber Law was familiarized. We are able to state cyber law as it's the chunk of the authorized techniques which deals with the web, Around the world Web, along with the legal things.

BhavnaArora (2016) - The world these days is actually experiencing an exponential growth of cyberspace. Nevertheless, India too has witnessed a major ascend in Internet pursuits and it's rather assertive to claim that such extraordinary growth of entry to info on a single hand leads to empowered company and people as well as on the additional hand additionally poses brand new problems to citizens and government. In order to come up with the cyber community safe is the demand of the hour. Putting up deterrent actions against cybercrime is actually crucial to national cyber security in protecting critical infrastructure of the nation in addition to for people.

Anil Kumar and Jaini Shah (2014) - With the era of globalization, computers, the Internet and mobile phones have grown to be a part of the everyday program of ours. As a consequence of this, internet processing info is actually made readily available on the web bringing in new threats in the type of cybercrimes. This kind of threats not just is available in faces that are different, though they likewise have a variety of delivery strategies making it hard for cyber professionals to locate a practical answer. Because of the high rates of threats, nations across the world have grown to be worried about the Netizens" online safety of theirs and also have applied a few

Acts of Parliament along with International Instruments. Nevertheless, majority of the laws continue to be in A Mother"s Womb that are in the procedure of evolution. There are many explanations why cyber-attacks are actually planned, as a few have considerable agendas tagged on them, while others are planned as pranks. This particular paper not just seeks to evaluate the political, social and economic consequences of cybercrimes in organizations but also recommends how one may be made aware and protect against cybercrimes in businesses as prevention is actually much better compared to medicine.

Tiwari Garima (2014) in her book "Understanding Laws–Cyber Laws and Cyber Crimes said the book comprises of nine parts, each managing a particular zone gave under the Information Technology Act, 2000. Different laws with respect to copyright, brand names, proof, and disciplines there under, have been examined, so that there is a complete comprehension of the law. The developing zone of electronic agreements, computerized marks, e-administration including e-courts and distributed computing have been independently managed and a short review on social networking websites has additionally been explicitly given. Significant offenses like hacking, data burglary, robbery, sexual entertainment, email misrepresentation and so on., have been expounded alongside the applicable case-laws and procedural issues.

Chandra (2013) assesses the issue of children's weakness to cybercrime through social networking destinations which has become a most loved distraction among them. Cyber tormenting and following are a reason for worry for guardians. Dr. Jitendra Nagpal, senior specialist, responsible for Institute of Mental wellbeing, MoolchandMedicity stated, "Around 60 to 70 percent cases of conduct issues in children are related with abuse of virtual space. Guardians should chat with their children and give them time as opposed to leaving them in the realm of PC.

Vadhera (2012) feels that social networking destinations have become a blend of feelings and thoughts which targets government, legislators and so forth. It is utilized some of the time to spread public disdain, disharmony and disappointment towards the government. Regardless of the Indian government's emphasis on networking goliaths to eliminate the frightful material from the net, they didn't react to the rehashed solicitations to obstruct the fiery substance which "affront Indian sensibilities". This made strain among government and social media organizations. In December 2011, a columnist held up a private criminal objection against 21 networking locales, in whose help he presented the materials which had deprecatory articles relating to different Gods. In January 2012, Indian Court cautioned these destinations that admittance to their sites will be impeded on the off chance that they neglect to eliminate frightful substance from their pages.

Godbole Nina (2011) in her book "Cyber Security" said this book is zeroing in on cyber dangers and cyber security, gives the truly necessary mindfulness in the hours of developing cybercrime scenes. There is Extensive treatment of significant theme i.e. cyber security to assist pursuers with understanding the ramifications of cybercrime. The book gives satisfactory direction on laws regarding cybercrime and cyber security considering the Indian just as worldwide situation. Mindfulness made through basic reasonable tips and deceives, instruct perusers to figure out how to abstain from turning out to be survivors of cybercrime.

Holt (2011) stresses on four significant sorts of cybercrimes, to be specific cyber trespass, cyber misdirection/burglary, cyber pornography and foulness and cyber savagery. He has talked about different criminological hypotheses in the light of changing patterns and examples of crime. He inspects hacking and its different structures. He additionally examined child pornography in the light of late legitimate turns of events. Moreover, he assesses the law which addresses cyber harassing and cyber following. In his perspectives more explores are required for making 'mindfulness' among the ordinary citizens who Google for anything and nearly everything.

Jaishankar (2011) implies the way that criminal equity actually needs appropriate and refreshed information concerning the cutting-edge cybercrime reality. His 'Space Transition Theory' is critical to get cybercrime. Obscurity has additionally become more criminogenic in virtual space. It has irritated Deviance and Criminal Subculture in Cyberspace. Social networking exploitation particularly juvenile exploitation has been related with Routine Activity Theory and Lifestyle Theory. Youngsters investigate new advances in view of the opportunity these innovations bring, yet it additionally makes them defenseless against online crime. In spite of the fact that cyber harassing is examined however inside a mental system and its social ramifications are not expressed.

3. Impact of E-crimes

E-crimes have emotional impact on the public in many ways. This consists of:

- Loss of online business and shopper trust in the advanced economy,
- The potential for basic foundation to be undermined influencing water gracefully, wellbeing administrations, national interchanges, energy dispersion, budgetary administrations, and transport,
- Loss of individual monetary assets and the ensuing passionate harm.
- Loss of business resources,
- Costs to government offices and organizations in restoring records of loan repayment, records and personalities,
- Costs to organizations in improving cyber security measures,
- Animating other crime, or
- Costs in time and assets for law implementation organizations.

4. Classifications of eE-crimes

Computer crime: Using of direct electronic activity that can assault security to acquire information and data wrongfully (Kumar, 2009).

High tech crime: An expansive scope of crimes that enter PCs, wrongfully infringing upon nation laws, or government laws. These crimes are finished by hacking, illegal tax avoidance, malware, provocation, electronic, and data fraud.

White collar crime: A crime carried out by an individual of decency and high social status over the span of his occupation to acquire cash. The well-known people who were indicted for

middle class are Kenneth Lay, Bernard Madoff, and Bernard Embers.

Cybercrime: It is a crime that is finished by utilizing PCs and the internet including anything from illicit downloading of music documents and games to taking great many dollars from online records. Additionally non-financial offenses, for example, making and circulating infections on different PCs or posting classified business data on internet through music and game records.

Cyber psychological warfare: Premeditated and politically persuaded assault against data, PC frameworks, PC projects, and information, which brings about brutality against regular citizen targets. Conceivable cyber psychological warfare targets incorporate the financial business, army bases, power plants, airport regulation focuses.

5. Technology: Cyber Vs. Real World Crime

Perhaps one way of viewing cybercrimes is that they are digital versions of traditional offenses. It appears that many cybercrimes could be considered traditional, or real world, crimes if not for the incorporated element of virtual or cyberspace. Indeed, many of these so-called cybercrimes can be easily likened to traditional crimes. For instance, identity theft can occur in both physical and cyber arenas. While these crimes may occur through differing mechanisms, in both circumstances the criminal intent (profit) and outcome (stolen personally identifiable information) are the same.

In the real world, a criminal can steal a victim's wallet or mail including documents containing personally identifiable information. In April 2011, two men were sentenced for leading a criminal enterprise that stole credit and debit cards from mailboxes in affluent neighborhoods in South Florida. The thieves then used the cards to make large purchases and cash withdrawals from the cards, costing victims $786,000. In another case, from September 2010, the leaders of a mail theft and identity theft ring were sentenced for stealing mail from mailboxes in more than 50 residences and law firms in Washington, D.C. The thieves took checks and documents containing personally identifiable information (PII) to cash forged checks at local banks.

In the cyber world, a computer hacker can easily steal this same PII—electronically rather than physically. In November 2011, a member of a Romanian criminal organization was sentenced for his role in a large scale bank fraud and identity theft scam. Dan Petri and co-conspirators installed high-tech skimming devices on bank automated teller machines (ATMs). These devices illegally captured victims' bank account information and PINs, which the fraudsters used to create duplicate cards and withdraw large sums of money, ultimately scamming victims out of more than $276,800. In another case, two defendants were sentenced in July 2010 for using peer-to-peer (P2P) software to search file sharing networks, stealing victims' account information and passwords. The defendants used this information to access victims' bank accounts and transfer funds to prepaid credit cards in the defendants' names.

6. Cyber Crime Scenario In India

The internet in India is developing quickly. It has offered ascend to new open door in each field like – amusement, business, sports, instruction and so forth. It is generally obvious that each coin has different sides, same for the internet, it utilizes has both bit of leeway and detriment, and one of the most hindrance is Cyber-crime. Cybercrime is rising as a genuine danger. Overall governments, police divisions and insight units have begun to respond. Activities to control cross fringe cyber dangers are coming to fruition. Indian police has started uncommon cyber cells the nation over and have begun instructing the staff.

The universe of Internet today has become an equal type of everyday routine and experiencing. Public are presently equipped for doing things which were not believable hardly any years prior. The Internet is quick turning into a lifestyle for a huge number of individuals and furthermore a method of living due to developing reliance and dependence of the humanity on these machines. Internet has empowered the utilization of website correspondence, email and a great deal of whenever anyplace IT answers for the advancement of mankind. In present age its fast development on Information Technology is encasing varying backgrounds. These specialized upgrades have made the change from record to paperless correspondence conceivable. While PC are intended to store favored data of Political, social, financial which carries gigantic advantages to the general public. The wide augmentation of an internet and Computer technology internationally has prompted heightening of internet related crimes. Lately, India has become significant spot for cyber criminals, who most programmers and different malicious clients perpetrate crimes through internet. As there as different sorts of cybercrimes these crimes are increasing at an alarming rate. India is positioned fifth in cybercrime among different nations. Under Indian law cybercrime doesn't have a particular definition under any Indian enactment one enactment that manages offenses identified with such crime is Information technology Act, 2000 which was later revised as Information Technology Act, 2008. So as to characterize such an offense, it very well may be done through reason for activity; it is a blend of PC and crime. In Asia district India has rank top two internet clients nation, so India is the quickest developing nation. Today internet turns into the foundation of social and financial world. Clients can get to the internet whenever from anyplace however through the internet numerous unlawful works may do. Today E-mail and website is the most effective method of data correspondence.

7. Conclusion

Cybercrime is actually viewed as simply a little threat or maybe trouble with the Government Authorities as it's normally placed at the conclusion of the list in Parliament. From, the above mentioned findings, it could be noticed that this's even more out of the truth as well as Governments should place far more reliance on overcoming that? crime? by stopping it properly. As the Governmental Authorities aren't bothered, therefore businesses also are taking it lightly. This means the techniques they normally use in fighting or perhaps fighting as well as monitoring these unwarranted cyber-attacks on the businesses aren't proportionate to the threats posed by the cyber criminals. The bigger risks of not solving the trouble is the fact that there aren't any sure stats on the issue, which means it's difficult to justify the improved powers that the Regulation of Investigatory Powers Act which have been given isn't for effect, hence be ineffective in coping with the computer system issues.The international treaties drawn by the authorities that deal with cybercrime are way too vague making

it ineffective in coping with the issue. What this means is that civil liberties will likely be impacted by the terms of the treaties since they can, conceivably, imply that everyone that has a laptop equipped with a modem or maybe an online connection might be suspected of becoming a cybercriminal. Efforts to outlaw the possession of hacking program may impact people, governments or organizations, whom wish to come up with the web safer which won't allow them to evaluate the methods of theirs, pointing that the legislation might provide or maybe do a lot more damage than good.The one certainty emerging out of this particular analysis is, with an exponential growth of cyber-criminal activity, this difficult struggle might be received by police authorities. This will need to be completed with the improvement of suitable mitigation techniques, along with a typical legal framework enacted by an established International Organization like The United Nations and put on harmoniously around the world by sharing information received from investigations conducted by different cooperation bureaus across the world.

References

1. Harjinder Singh Lallie, et al (2020) – "Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic", arXiv:2006.11929v1 [cs.CR] 21 Jun 2020
2. Pujari, Vinayak & Patil, R & Dalvi, Rohit. (2020). CYBER CRIME & CYBER LAW'S IN INDIA.
3. Bhavna Arora, Exploring and analyzing Internet crimes and their behaviours, Perspectives in Science, Volume 8,2016, Pages 540-542, ISSN 2213-0209, https://doi.org/10.1016/j.pisc.2016.06.014. (http://www.sciencedirect.com/science/article/pii/S2213020916301537)
4. Kumar, Anil & Shah, Jaini. (2014). The Threat of Advancing Cyber Crimes in Organizations: Awareness and Preventions. International Journal of Advanced Research in Computer Science. Volume 5, No. 8,. 84-91.
5. Tiwari Garima (2014) in her book "Understanding Laws–Cyber Laws and Cyber Crimes", http://www.bookskhoj.com/product/quick-reference-guide-ganda-series-civil-procedure-code-limitation-act-2014-s-r-rosedar/
6. Chandra, Neetu (2013). Social Networking sites a concern for Parents. India Today, April 1, 2013.
7. Vadhera, Sharad (2012), Fate of Social Networking Sites in India. Kan and Krishme, Global Advertising Lawyers Alliance.
8. Godbole, N., Belapure, S., (2011) Cyber Security: Understanding Cybercrimes, Computer Forensics and Legal Perspecives. New Delhi. Wiley India.
9. Holt, Thomas J (2011), Crime Online : Correlates Causes and Contexts. Durham, Caroline Academic Press, USA .
10. Jaishankar, K.(2011). Cyber Criminology : Exploring Internet Crimes and Criminal Behaviour. CRC Press: Taylor and Francis Group,USA.

