CYBER ATTACKS: AN ECONOMIC IMPACT

By Nishtha Vaswani
From Symbiosis Law School, Hyderabad

ABSTRACT

Virtual world has become more familiar to people than the physical world we live in, but the same is not with the crimes that happen in the technological sphere. There is a high amount of ignorance that cyber-attacks face which in turn harms the data of people present in their technological system. This harm extends not only to individuals but to nation's security also and thus has become a national security issue which affects privacy of a nation along with other factors. These other factors include the economy of a nation also, for which surveys are conducted to measure the impact of cyber-attacks on an economy, however there are not many major steps taken to raise awareness about the same.

This study has been conducted to generate a comparative analysis between the awareness that the various business houses have and individuals have. The questionnaire was circulated between IT departments of small, medium and large scale businesses which has been quantitatively compared with responses received in surveys done with various individuals. Information regarding the precautions, awareness of type of cyber-attack and impact of it on business is also drawn upon. The conclusion and suggestions provided in the research paper are based on this small survey conducted which reflects an important issue. Though the survey sample is small but it helps in considering the gravity of lack of awareness in society pertaining to cyber-attacks and what measures can be taken to improve the same.

Key words: Cyber-attacks, Economical impact, Business houses, Awareness

1. INTRODUCTION

Cybercrime and cyber-attack are two phrases which are perceived similar to each other by the majority of people, however such is not the case. Cybercrime is a crime which takes place with the help of a computer through the Internet or Cyberspace, the computer may be the target or a tool to achieve the completion of the crime.[1] In other words, cybercrime can be perceived as a traditional crime but with the use of cyberspace or computers.[2] Whereas, a cyber-attack can be construed as an attempt to enter into the computer systems or servers through unauthorized access with malicious intent to either steal, alter or hamper any information available on the respective system.[3] Though there is a slight line of difference between cybercrime and cyber-attack, there is still no uniform definition available as the interpretation of these two concepts varies from nation to nation. However, this paper will cover the aspect of cyber-attack only.

Cyber-attack has grown as phenomenally as the development of digital computer systems in 1940's with mere difference being, in early days people who used to commit theft of data were the ones who were well-acknowledged with the language of computers and had access to the same because only binary

[1] Yerra Rao & Hemarj T.C.Panda, *Effect of Cyber Crime Indian Economy*, 1 IJRTS 4–7 (2014).
[2] Id.
[3] Daniela Oliveira, Cyber-Terrorism & Critical Energy Infrastructure Vulnerability to Cyber-Attacks, 5 Envtl. & Energy L. & Pol'y J. 519 (2010).

language was used to run a computer with size of a room.[4] The terms "cybercrime" or "cyber-attack" or "hacker" were not developed till that period, it was called "theft" or "computer crime" till the 1960's.[5] The majority of the world was not aware about the structure of the computers, thus the thought of committing crime on computers was a far cry; this helped in narrowing down the criminals who hampered data stored on a computer. But, with the passing time, the intention to provide benefit of technology to everyone the amount of cyber-attacks grew like a fire and gained worldwide attention. The "Digital Equipment Corporation (DEC)" developed a computer and provided it on a timely basis for use by the public, the data of various organizations was available openly and accessible to many. The term "hacker" gained recognition through the first group of hackers called the "Tech Model Railroad Club" in 1961 who interrupted the data of the "Massachusetts Institute of Technology (MIT)" with the purpose of enjoyment not for any monetary gain or leaking information etc. MIT used the computer provided by DEC.[6] Hacker was considered to be a person who was well versed with computer technology and mastered the art of handling various functions of the same. The inference of criminal implication or the malicious connotation from the word "hacking" became evident in 1970's when the digitized phone systems were tampered to make free calls, this was done by Joe Engressia on Bell Telephone Company by whistling in a certain pitch which changed the setting of the automated calling system. "Phreakers" was the term introduced for the persons hacking the telephone system and "Crackers" for the people who tampered the security of a system.[7] The more acquaintance and availability of the technology provided a platform for cyber-attacks and due to lack of legislation there were no serious punishments imposed. People did not even have sympathy for the telephone companies who suffered a lot of loss due to these kinds of disruptions in the systems.[8] There have been hacker and group of hackers like, "Legion of Doom" which was a group of hackers started by a person because of rivalry with the company he worked in and "Fry Guy" who obtained keys to enter into McDonald's system and increased salary of few of his friends in 1980's, "Masters of Deception" who were involved in harming the telephone systems, mini-computers etc. during 1990's, the "Operation Shady Rat" which was started in 2006 and has around 71 cyber-attacks till now, the "Sony Pictures Hack" of 2014 done by "Guardians of Peace" where a lot of company's information was leaked[9], these are only few mentioned, there have been numerous cases every decade and a lot of economic harm has been faced in every attack, but the mention of how much is provided in only some cases.

The loss of profit or the economic impact on the companies was present four decades ago similar to today, but formerly it was not given much importance but presently is has become essential to provide information regarding economic impact of cyber-attacks because

[4] DEBRA LITTLEJOHN SHINDER & MICHAEL CROSS, SCENE OF THE CYBERCRIME (Elsevier) (2008) (pp.41-44)

[5] Id.

[6] Id.

[7] VANNESA PITTS, CYBER CRIMES: HISTORY OF WORLD'S WORST CYBER ATTACKS (Vij Books India Pvt Ltd) (2017)

[8] Id.

[9] BRUCE MIDDLETON, A HISTORY OF CYBER SECURITY ATTACKS: 1980 TO PRESENT (CRC Press) (2017)

money has become essence of everything, thus making of proper legislation is required to overlook cyber-attacks which affect not only individual but whole of a nation politically and economically by intruding the cyberspace of a nation and tampering the data present there. In India, the recent cyber-attacks which have caused monetary losses are, the 2018 Cosmos Cooperative Bank Ltd.'s ATM hacked in Pune which led to transfer to Rs. 94.42 crores by the hackers, similar attack was done on Canara Bank's ATM wherein 20 lakh rupees were stolen, the UIDAI Aadhar system was also hacked in 2018 which led to leaking of information like, Aadhaar, PAN and mobile numbers, bank account numbers, IFSC codes etc. and was available to people on WhatsApp at mere amount of Rs. 500.[10] Recently in June 2020 there was a threat remitted at "Jammu and Kashmir Power Development Department" on four of its servers at the data center, however it was resolved later.[11] In the fourth quarter of 2019, India ranked 32nd in the list of being more vulnerable to cyber threats which increased to 29th rank in the first quarter of 2020, according to the survey conducted by Kaspersky Security Network.[12] It has been mentioned by various news articles that there were more than 40, 200 cyber-attacks by China trying to interfere in the cyberspace of India and there was a surge to have strong firewalls to resist the same.[13] Cyberspace has become such a critical arena which is used to damage a country's economy, either by obtaining confidential information or destroying essential information, this happens on a macro level. But, on micro level the cyber-attacks which are faced by individuals are done in name of vengeance or intrude someone's privacy or with some personal agenda, the main point is many a times people are unaware that their data encrypted in cell phones or computers is being accessed by someone which is because of lack of awareness. This research will show the awareness among people and how ignorant people have become as technology has become part and parcel of the quotidian world.

There are legislations present like the Information Technology Act of 2000 and "Information Technology (The Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules 2013 (the CERT Rules)", which established a "Computer Emergency Response Team" (CERT-In) to deal exclusively with recording the movements in cyberspace related to crime and other threats.[14] There are provisions which provide punishments for committing a crime in the cyber world, but do people are aware about

[10] 5 Biggest Cyber Attacks in India | Everything You Need to Know | Kratikal Kratikal Blog, https://www.kratikal.com/blog/5-biggest-cyber-attacks-in-india/

[11] J&K Power Department Data Centre Targeted in Cyberattack, Threat Contained: Official News18, https://www.news18.com/news/india/jk-power-departments-servers-targeted-in-cyberattack-threat-contained-official-2689363.html

[12] 37% increase in cyberattacks in India in Q1 2020: Report - ET CISO ETCISO.in, https://ciso.economictimes.indiatimes.com/news/37-increase-in-cyberattacks-in-india-in-q1-2020-report/75962696

[13] Chinese hackers attempted 40,000 cyber attacks on Indian web, banking sector in 5 days India Today, https://www.indiatoday.in/india/story/chinese-hackers-attempted-40-000-cyber-attacks-on-india-1692088-2020-06-24

[14] Cyber-laws-in-India.pdf, https://www.latestlaws.com/wp-content/uploads/2015/05/Cyber-laws-in-India.pdf

the same, this research will bring out this information through survey and provide suggestions regarding what measures or steps can be taken to improvise the knowledge about cyber-attacks in common people. An analytical comparison will be drawn between the responses received from the IT departments of various business houses and different individuals. This will help in understanding whether an amateur public who does not have deep knowledge about working of technology is aware about the dark side of cyberspace comparatively to professionals who are dedicated to handle the technology of different companies. Also, whether after facing cyber-attacks what have been the consequences faced financially by both business houses and individuals.

2. RESULT OF SURVEY

There were two questionnaires circulated, one for the people who work in IT departments of various business houses including large scale, medium scale and small scale businesses, other for individuals who do not work or are related to the IT industry. The names and identity of the respondents has not been disclosed because of confidential reasons. There were similar questions asked in both the questionnaires which made it convenient to compare the results of both surveys. The sample space of both the surveys is not the same but it can still be rationalized through comparison. There were 165 responses recorded in the survey conducted for the individuals and 100 responses from the survey conducted for business houses.

2.1 BUSINESS HOUSES

Sixty three people of IT departments of large scale business houses responded and thirty seven of medium and small scale businesses (Fig. 3.1.1). Out of the total percentage only 36% of them faced a cyber-attack in their technological system (Fig. 3.1.2) and only 12% had faced economic loss because of the attack (Fig 3.1.4). It can be generally construed that the IT departments of at least businesses or companies will take precaution to save their system from facing cyber-attacks or protecting their confidential information, but in this survey 8% of them replied negatively when asked about whether they take precautionary actions to protect their technological system from cyber-attacks (Fig 3.1.5). Though the number is very less, but even this can hamper a security and confidential information of a business even if it is a small business, cyberspace and information stored in it is at very vulnerable situation because use of technology has become very prevalent and paperwork is reduced, and a person is just a password away or whatever method he uses to enter into system to get information stored in the computer or device whatever a business house uses. The people who faced cyber-attack mentioned eleven types of attacks they faced which includes, phishing, hacking, ransom ware, data theft/loss, malware, locky, Trojan virus, gray ware, botnet and DDoS i.e. distributed denial of service (Fig 3.1.3). Phishing is the act of obtaining confidential or sensitive information like credit card numbers or password or account details etc. carried out through sending mass emails or messages to users to update their personal information for a certain apparent legitimate website and the users believing so without due cross-checking fall victim to such attacks and lose their confidential or sensitive information.[15] The phishers mainly attack the users of e-commerce or online banking and commit monetary fraud transactions post receiving information, which results in financial losses and theft of information or data.[16] Hacking has various definitions prevailing and developing but a definition with combination of all the features, it can be construed as act to enter into cyberspace of certain computer systems and harm the information present there with malicious or an illegal intent, though not every attempt is for sabotaging information sometimes people do it for fun.[17] Malware is a wider term which means a software which is created to harm a computer system without the consent of the user[18], the other attacks which have been mentioned by the respondents which are ransom ware, Trojan virus and locky, all come under the purview of malware. Trojan is a kind of malware which in nature is a program and it makes copies of itself in the computer of the victim to steal information which happens automatically and infects the system.[19] Ransom ware is also a kind of malware which locks the screen of the system or encrypts files present in the device and forces the victim to pay a certain ransom amount to get the decrypt key or to access the system normally, whichever the case may be.[20] Locky is type of ransom ware which makes it a kind of malware also, however locky had been created recently around 2013, it is disguised as email or invoice receipt alike to malware, but when it is downloaded the files of the system are encrypted because macros are enabled and Bit coin which is a crypto currency is demanded to be paid in order to decrypt the files.[21] The category of fraud mails and data theft/ loss will be covered under malware only, as mails are the tool to carry on the act of data theft or loss whichever is the case. Gray ware is a kind of software which tracks habits and patterns of the victim while using the online data and it is desired to collect information which is sensitive and confidential, it can happen through showing different pop-ups or advertisement while using internet[22], the consumer may feel that the pop-ups are related to what they desire to search and get, however it is their search pattern which is being tapped to get into their system for generating confidential information. Botnet is a term which is derived from the combination of two words viz. Bot i.e. Robot and Net i.e. Network, the devices which are connected to the internet and are infected are called Botnet, these devices are controlled by a Botmaster or Botherder through a server.[23] When a system becomes a part of the Botnet through use of a code, it can either be a laptop or computer or mobile phone which uses the internet, then the Botmaster can commit any act like fraud or data theft etc. on that system without the knowledge of the user.[24] Denial of Service is a kind of attack which disables the user to access certain online resources or

[15] Cheman Shaik, *Counter Challenge Authentication Method: A Defeating Solution to Phishing Attacks*, 10 IJCSEA 1–8.

[16] Id.

[17] Seda Duman, *Integration of Hacking Mindset and Practice to Industrial Design Education*, 8 OLAD 137–149 (2020).

[18] Nirav Bhojani, *Malware Analysis* (2014).

[19] Id.

[20] S.Mahmudha Fasheem, P. Kanimozhi & B. Akora Murthy, *Detection and Avoidance of Ransomware*, 5 IJEDR 590–595 (2017).

[21] Id.

[22] Zhongqiang Chen et al., *Evaluating Grayware Characteristics and Risks*, 2011 JCNC 1–2 (2011).

[23] Shahid Anwar et al., *A Review Paper on Botnet and Botnet Detection Techniques in Cloud Computing* (2014).

[24] Id.

any resource by creating an online traffic which makes the system more vulnerable and an easy target to perform other cyber-attacks.[25] Distributed Denial of Service is similar to Botnet wherein mass of systems are taken under control of the attacker through coding or encrypting certain files which makes the system easily available for exploitation on hand of the attacker for disrupting the use of device for internet purposes through creating a traffic and then it is used for various malicious purposes.[26] These are various kinds of cyber-attacks that were mentioned in the survey except Denial of Service, but it is explained as it is a prevalent form of cyber-attack in cyberspace.

Figure 2.1.1

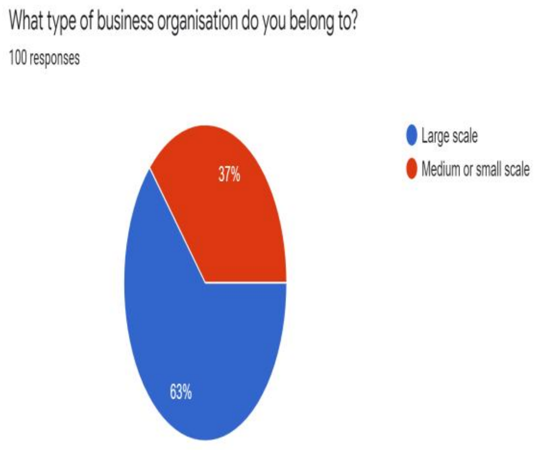


Figure 2.1.2

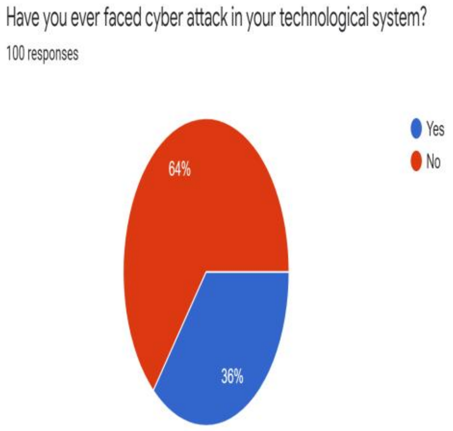


Figure 2.1.3

TYPE OF CYBER-ATTACK FACED	NO. OF RESPONSES
1. PHISHING	18
2. HACKING	5
3. RANSOMWARE	5
4. DATA THEFT/LOSS	3
5. FRAUD MAIL	3
6. MALWARE	2
7. LOCKY	2
8. TROJAN VIRUS ATTACK	1

[25] K. Munivara Prasad, Dr A. Rama Mohan Reddy & Dr K. Venugopal Rao, *DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms - A Survey*, GJCST (2014), https://computerresearch.org/index.php/computer/article/view/1081

[26] Id.

9. GRAYWARE	1
10. BOTNET	1
11. DDOS	1

Figure 2.1.4

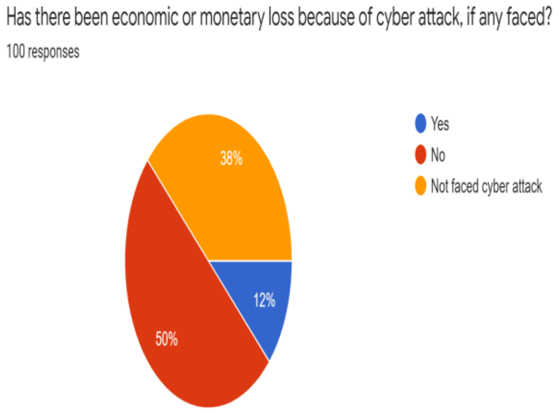
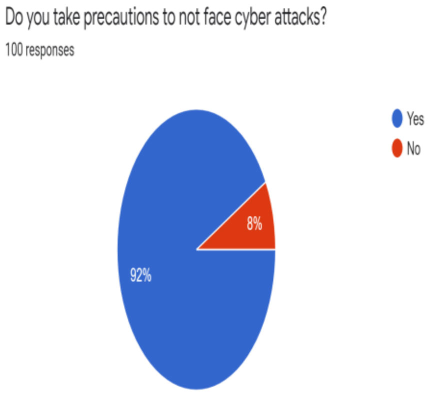


Figure 2.1.5



2.2 INDIVIDUALS

There were 165 responses recorded, out of which 47 of them responded positively for facing cyber-attack (Fig 3.2.1), however only around 28% of the total were aware about the type of cyber-attack they faced and 13% were not (Fig 3.2.2) and only 12 people of total sample space had faced economic loss because of the attack (Fig 3.2.4). When questioned about the precautionary actions taken to protect the technological system, 138 responded affirmative and 27 in negative. This reflects that though people are well acquainted with the technology and its negative side and vulnerability of data stored in cyberspace, even then few of them are casual about its security. The types of cyber-attacks mentioned by the respondents were hacking, phishing and malware (Fig. 3.2.3), mostly the online social accounts like Instagram and Facebook were hacked. The terms hacking, phishing and malware have already been discussed under the head of Business Houses.[27] The hacking involved with the individuals is different from the hacking faced by business houses, latter face financial losses if there system is hacked because it has financial information whereas in case of individuals where Instagram account or Facebook account is hacked, they maximum times will not face monetary loss but a loss of reputation or feel embarrassed if their account is used maliciously by the hacker, such acts are atrocious and may result into undesirable consequences. These accounts are through cracking the passwords of the accounts and it is seen that for such acts some professional experts are not required, even amateur people may hack accounts through obtaining passwords and misuse it.[28] Therefore, it is advised to not save the password on devices for any account as if someone gets the access then it may be misused, which either may result in financial losses or reputation or social image of a person being affected. Like, recently in July, 2020 Twitter Accounts of various famous

[27] For detailed information, see supra 15, 17 and 18.

[28] Seda Duman, supra 17.

and prominent personalities were hacked and fake posts were made for Bit coin amounts being multiplied and sent back to the people who deposit a certain amount on the given address in post.[29] This shows that every person is vulnerable to such hacks and attacks on their accounts, thus there is a need of proper safety and steps taken for awareness among people.

Figure 2.2.1

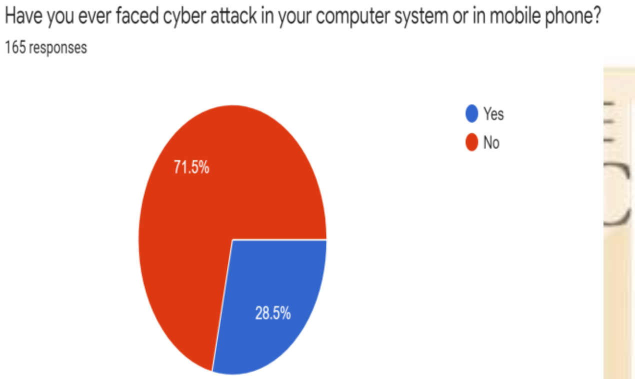


Figure 2.2.2

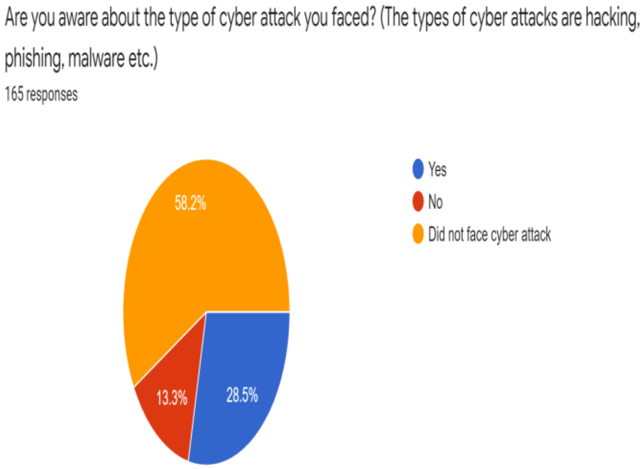


Figure 2.2.3

TYPE OF CYBER-ATTACK FACED	NO. OF RESPONSES
1. HACKING	22
2. PHISHING	8
3. MALWARE	5

Figure 2.2.4

[29] India Today Web Desk New DelhiJuly 16, 2020UPDATED: July 16 & 2020 10:35 Ist, *Twitter hacked in major breach, accounts of Obama, Biden, Gates, Bezos, Musk, others taken over*, India Today , https://www.indiatoday.in/world/story/twitter-accounts-barack-obama-bill-gates-joe-biden-jeff-bezos-elon-musk-1701037-2020-07-16

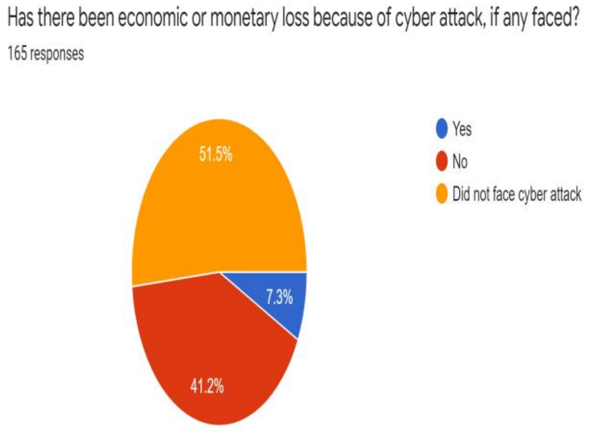
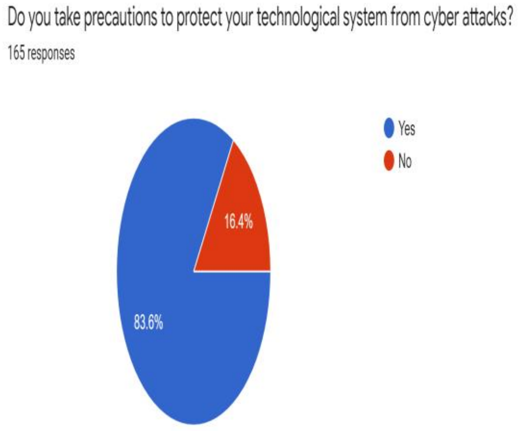


Figure 2.2.5



2.3. COMPARISON OF BUSINESS HOUSES AND INDIVIDUALS

The comparison of amateurs and professionals of IT department, though can be considered as a rational comparison because latter has in-depth knowledge of technology than former, but even then when analyzing behavioral pattern of both, there are certain common points that can be noted. Like, the economic losses have been faced by 12 people in both sample spaces, this shows not only ordinary people but even technological systems of experienced professionals are vulnerable to such cyber-attacks even after taking due precaution. It is normally expected from IT professionals to act diligently in protecting technological system from viruses or cyber-attacks, but 8 people out of total sample space denied when asked about precautions being taken against cyber-attacks, out of which 6 belong to medium or small scale business and 2 to large scale business, though the number is less but even then such omission of not protecting technological systems, makes the information of company or business present in cyberspace at high risk and easy target of cyber attackers. The information can be used maliciously and a business may lose all its monetary or financial assets if information about bank accounts get leaked because majorly the attempts are for theft of money and for data. Therefore, there can be various conclusion drawn, like either there is unawareness among people about how to protect their system from cyber-attacks or they are deliberately doing so to make information vulnerable or they do not care about cyber-attacks because they have never faced one, these are simple assumptions, the actual reason may differ from individual to individual. There is a need for proper knowledge and awareness to be raised among ordinary people as well as professionals with regard to cyber-attacks and how to protect their technological systems from such attacks.

3. CONCLUSION AND SUGGESTIONS

In India, the only legislation which deals with cyber related acts is Information Technology Act, 2000, but even in this Act there is no proper definition of cyber-attacks, the basic is need is to demarcate the difference between cyber-attacks and cybercrimes, because the connotation of crime adds a malicious intent to the act, which is not the case in attack. Also, many times people ignore small breaches of privacy which is done by online websites or other softwares, the tracking of behavioral pattern and showing advertisements of the search terms which have been used by a user on a device is also a breach of privacy, because not every person would want their searches to be known, though online websites or softwares ask to accept or deny the privacy policy but if a user denies the websites does not open nor do the softwares, they tempt the users of accept their policies if they want to access the website or software, whatever the case may be. Thus there is a need for stricter laws and proper definitions of important terms in India because the importance of technology has grown in this decade and in future will grow more as paperless work is being preferred more and every information is present in the new world called cyberspace.

*****