CYBERCRIME, ICT AND THEIR IMPACT ON CONSUMER BEHAVIOR

Parul[*]

ABSTRACT:

The Internet has revolutionized the computer and communications world like nothing before and has bestowed us with many advantages possible only because of it. With the evolution of the Internet, along came another revolution of crime where the perpetrators commit acts of crime and wrongdoing on the World Wide Web. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual. These attacks have become a bottleneck for people as well as industrialists and online shops. Due to fast growing world we cannot deny the need of computers and internet for our day to day business transactions and personal use. At the same time, scenario has become menacing for internet users and online shoppers. Therefore, we have to be aware of what kind of security breaches can happen while using internet and what are possible ways of getting rid of these attacks. The article provides a brief review about cybercrime, types of cybercrime, factors responsible and impacts on consumer behavior.

Keywords: cybercrime, ICT, online, internet, attacks, consumer, behavior

IJMRA

[*] Assistant Professor in Computer Science, GDC Memorial College, Bahal (Bhiwani)

1. Preface to Cybercrime

As computer has become central to commerce, entertainment and governance activities, the cybercrime has increased tremendously from past few years especially because of the use of internet. Cybercrime or computer-crime is any crime that involves a computer and the internet to perform illegal tasks such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. More and more criminals are exploiting the speed, convenience and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual. Cyber attacks may have some motivation behind it or may be processed unknowingly. The attacks those are processed knowingly can be considered as the cybercrime and they have serious impacts over the society in the form of economical disrupt, psychological disorder, threat to National defense etc. Restriction of cybercrimes is dependent on proper analysis of their behavior and understanding of their impacts over various levels of society (Saini et al, 2012). Internet has provided opportunities to cyber criminals. The nature of some ‘traditional’ crime types has been transformed by the use of computers and other information communications technology (ICT) in terms of its scale and reach, with risks extending to many aspects of social life, such as(Cybercrime: A review of the evidence, 2013):

- Financial transactions;
- Sexual offending;
- Harassment and threatening behavior; and
- Commercial damage and disorder.

The first cybercrime was noted in 1820 by Joseph-Marie Jacquard, a textile manufacturer in France which produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. (Introduction to cybercrime, 2015)

IJMRA

One of the reasons behind increase in cybercrimes is the vulnerability of computers. Now days, computers have become vulnerable because of the following reasons (Cybercrime worldwide, 2011):

- **Capacity to store data in comparatively small space:** The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier.
- **Easy to access:** The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.
- **Complex:** The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.
- **Negligence:** Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system.
- **Loss of evidence:** Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

2. Genres of Cybercrime Attacks

There are a number of forms of cybercrime attacks now days. We are discussing a few of them below:

- **Hacking –** It is the act of gaining unauthorized access to a computer system or network and in some cases making unauthorized use of this access. Hacking is also the act by which other forms of cyber-crime (e.g., fraud, terrorism, etc.) are committed.

- **Online Pornography -** There are laws against possessing or distributing child pornography. Distributing pornography of any form to a minor is illegal. The Internet is merely a new medium for this `old' crime, but how best to regulate this global medium of communication across international boundaries and age groups has sparked a great deal of controversy and debate.
- **Credit/Debit Card Fraud:** It is the unauthorized use of a credit/debit card to fraudulently obtain money or property. Credit/debit card numbers can be stolen from unsecured web sites, or can be obtained in an identity theft scheme.
- **Piracy –** It is the act of copying copyrighted material. The personal computer and the Internet both offer new mediums for committing an 'old' crime. Online theft is defined as any type of 'piracy' that involves the use of the Internet to market or distribute creative works protected by copyright.
- **Assault by Threat** – Threatening a person with fear for their lives or the lives of their families or persons whose safety they are responsible for (such as employees or communities) through the use of a computer network such as email, videos, or phones.
- **Cyber vandalism** - Damaging or destroying data rather than stealing or misusing them (as with cyber theft) is called cyber vandalism. This can include a situation where network services are disrupted or stopped. This deprives the computer/network owners and authorized users (website visitors, employees) of the network itself and the data or information contained on the network
- **Denial-of-service (DoS**): Denial-of-service attack is a special form of cyber attack that focuses on the interruption of a network service. This is achieved when an attacker sends high volumes of traffic or data through the target network until the network becomes overloaded ("Denial-of-Service"). Think of a man juggling; he may be able to juggle quite well when using three or four balls, but if someone throws more balls into the fray and he tries to continue juggling with an increasing amount of balls, he may lose control and drop them all. This is essentially what happens when a network becomes overloaded.
- **Malicious Programs/Viruses:** Viruses and malicious programs can potentially impact a massive amount of individuals and resources. These programs are intended to cause

electronic resources to function abnormally and may impact legitimate users access to computer resources

2.1 Percentage of Attacks Encountered

The protectors of cyber world whether government or any private agency, all of them are putting lot of efforts to eradicate cyber attacks and their causes. It has been found a tremendous increase in the rate of cyber attacks due to the vulnerability of computer and information technology. This statistic shows the types of cybercrime attacks most commonly experienced by companies in the United States. During a 2014 survey of 60 U.S. companies, it was found that 97 percent of respondents had experienced malware attacks as shown in Figure 1. The most common type of attacks were viruses, worms and Trojans (The Statistics Portal, 2014)

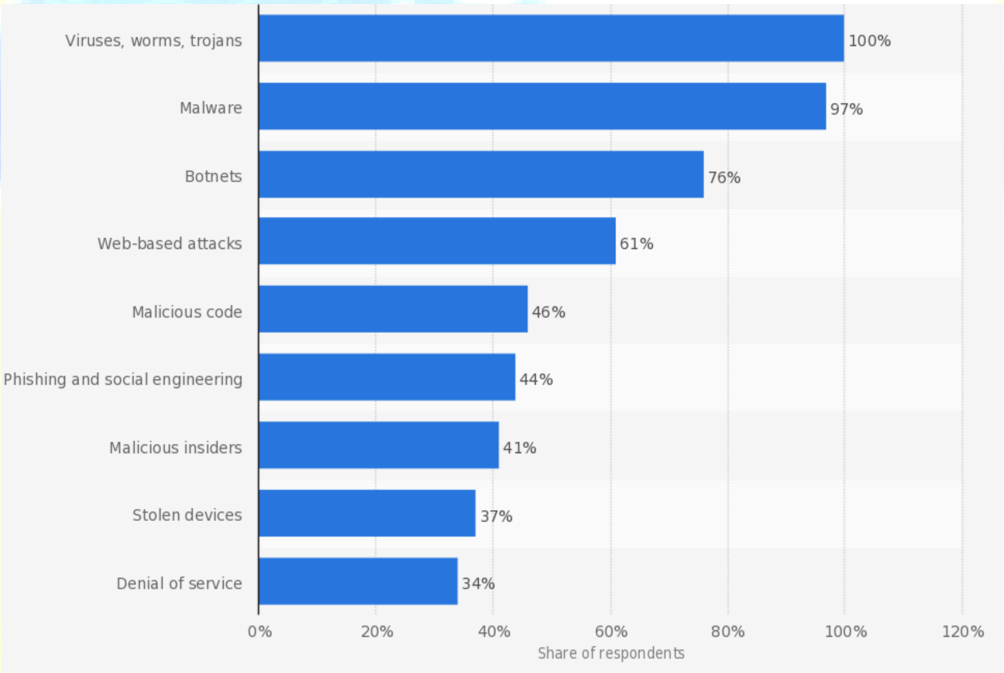

Figure 1 Percentage of attacks encountered

3. ICT and Cybercrime

Information and communication technology is a combined term used for many of the constituents of today's world including telecommunications (telephones, mobiles, wireless signals), computers, enterprise software, middleware storage and other audio-video aids which makes it easier to exchange and manipulate information. Although, there are a great number of advantages earned from ICT but we cannot neglect its obstructive impacts on the cyber world that are being faced by large organizations to a common man. Such crimes may threaten a nation's security and financial stability. Cybercrime can simply be explained as crimes carried out with the aid of a computer system against an individual, organization or a nation. (Hassan, 2012).

In present scenario, the most important use of internet or we can say ICT is for business purposes. Large organizations to smaller ones, all of them are relying on internet for their business transactions, buying, selling and paying bills and for these tasks to be accomplished a lot of information is shared via internet. This information, whether it is bank account details, ATM pins or images acts as an input for hackers.

3.1 Factors Behind Making ICT Obstructive

ICT is blend of all the technologies that science can give us; still a scenario has been developed where technology is used for purposes other than that for which they were originally developed. Here are some of the factors which can be considered responsible for ICTs negative impacts:

3.3.1 Ignorance

There is no doubt that due to emergence of ICT and techniques the rate of progress in every sector is increased. Information and communication technology is a vast field encompassing virtually all technologies that can store, receive or transmit signals electronically. With electronic devices so tightly wound into the fabric of modern society, the advantages and disadvantages of ICT use may not be immediately apparent. It is not necessary that an entrepreneur who is holding a business might be fully computer literate or he might know every aspect of security. In that case, that entrepreneur is very much vulnerable to security attacks. These attacks may cause fraudsters to gain access to your personal details, which could result in you or your business losing money and reputation.

3.3.2 Digital Diversity

The digital diversity generally refers to differences between individuals in likelihood of accessing and using the information technologies, specifically the Internet resources. The phrase of digital diversity is seen as well as due to demographical, socio-cultural, psychological and political characteristics. The crucial include income, education, gender, age, race/ethnicity, caste, infrastructure indicators, pricing regulatory quality etc. (Parul, 2014). To use computer or Internet some sort of skill/ competence is required to locate content online effectively and efficiently (Hargittai, 2002). These vary due to age, experience, gender and educational standard. And because of this diversity in technology, computer illiterate persons are becoming major victims of cybercrime attacks.

3.3.3 Hackers Attitude

An ethical hacker is a computer and networking expert who systematically attempts to penetrate a computer system or network on behalf of its owners for the purpose of finding security vulnerabilities that a malicious hacker could potentially exploit. (Ethical hacking, 2015), but what if the person involved in ethical hacking may become dishonest towards their organization and may allow the crucial details to be seen by some unauthorized persons.(Passi, 2014) Ethical hackers may send some malicious code or virus to the system which can destroy the whole network. So, it depends upon the individual's attitude towards his organization or oneself that he will commit such a dishonest task or not.

3.3.4 Shoppers Behavior and Mode of Payment

There are two kinds of shopper's in India, one is metropolitan shoppers and another is non-metropolitan shoppers. As documented by Zia and Manish (2012), shoppers in metropolitan India are driving eCommerce: These consumers are primarily buying travel, consumer electronics, and books online. And although spending per online buyer remains low, some 59% of online consumers in metropolitan India already make purchases online at least monthly. Consumers in nonmetropolitan areas will also help fuel growth; unlike online consumers in cities, they are more likely to shop online for goods that are unavailable at local stores. Zia and Manish (2012) estimated that eCommerce retailers in India are expanding their offerings to the online population outside metropolitan India and are investing heavily in the infrastructure to support these cities. In these cities, the mode of payment plays an important role against cybercrimes related to shopping. If a shopper shops by opting COD (Cash on Delivery) then he will be supposed to pay only after receiving his ordered product but if he shops by choosing options like debit card or credit card he has to input his bank account related details. In the later case, shopper's details leave him prone to online credit card theft.

4. Effects of Cybercrime on Consumer Behavior

In the above section we have discussed cybercrime, factors responsible for it and have found out that it is not just the technology that is wholesomely responsible for cybercrimes, it is also consumer's attitude, his technical knowledge responsible for breaches in cyber security. The results are that consumers are less likely to shop again, to bank online again, and to provide personal details. According to a survey by Special Eurobarometer 404 by European Commission the actions respondents are most likely to take are installing anti-virus software (46%) and not opening emails from people they don't know (40%). Other changes include being less likely to give personal information on websites (34%), only visiting websites that they know and trust (32%), only using their own computer (26%) and using different passwords for different sites (24%). Other actions are mentioned by around one in six respondents: 17% say they are less likely to buy goods online and 15% are less likely to bank online, while 16% have changed their security settings. In addition, 6% have cancelled an online purchase because of suspicions about the seller or website. However, 18% of respondents say they have not made any changes because of concerns about security issues (European Commission, 2013). This survey was conducted on 15+ age groups.

5. Conclusion

Today, because of dependence on information and communication technologies (ICT), especially the Internet, for delivery of services and operations, one of the biggest challenges the world faces is that of cyber security. The digital age has changed every aspect of our daily lives and at the same time brought about new global threats, which require a holistic approach to tackle them. These global threats cover a wide spectrum of crimes and every day their number and their impact on society increase. Such crimes could include attacks against computer data and systems, identity theft, the online distribution of child sexual abuse images, attacks against online financial services or critical infrastructures, e-mail scams and the deployment of malware. In this article we have studied a brief review of cybercrime, its genres, possible factors responsible for ICT's involvement in cyber attacks and impacts of cyber attacks on consumer behavior. It has been found out that many individuals or firms are facing threats of cybercrime from small cities to metropolitan cities. Many of the consumers or e-shoppers have reduced their rate of buying products from online stores. It has become a burning issue in cyber-space. Though government has made many laws against cybercrime but awareness about these crimes is essential. If people pay attention to measures against these attacks, it is trouble-free to eradicate the same.

6. References

[1] Cybercrime worldwide .(2011). Retrieved from https://sites.google.com/site/cybercrimezbd/reasons-for-cyber-crime on 15 March 2015

[2] Ethical Hacking. (2015). Understanding the Benefits, Goals and Disadvantages. Retrieved from http://www.brighthub.com/internet/security-privacy/articles/77412.aspx on 15 March 2015

[3] European Commission. (2013). Special *Eurobarometer 404 CYBER SECURITY REPORT*, 2013. Retrieved from http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf on 16 March 2015

[4] Hargittai, E. (2002). Second-level digital divide: Differences in people‘s online skills. *First Monday*, 7(4)

[5] Hassan A. B., Lass F. D. and Makinde J. (2012). Cybercrime in Nigeria: Causes, Effects and the Way Out. ARPN *Journal of Science and Technology ©2011-2012*, ISSN 2225-7217, 2(7)

[6] Introduction to cybercrime. (2015). Retrieved from http://www.inf.tsu.ru/WebDesign/libra3.nsf/317094d25b4410c6c62571f5001deba4/3b47f7a6821452fdc62572040016d843/$FILE/cybercrime.pdf on 15 March 2015

[7] McGuire, M. & Dowling, S. (2013). Cybercrime: A review of the evidence, Summary of key findings and implications. *Home Office Research Report 75*, Retrieved from https://www.gov.uk/government/uploads/...data/.../horr75-summary.pdf on 15 March 2015

[8] Parul. (2014). Correlates of the Digital Diversity in the Information Age: A Bird's Eye View. *International Journal of Computer Applications*, ISSN 0975 – 8887, 106(9):41-53

[9] Passi, A. & Sharma, P. (2014). Compressive Study on Ethical Hacking . *International Journal of Emerging Research in Management &Technology*, ISSN 2278-9359, 4(1)

[10] Saini, H, Rao, Y, S & Panda, T, C. (2012). Cyber-Crimes and their Impacts: A Review. *International Journal of Engineering Research and Applications (IJERA)*, ISSN 2248-9622, 2(2): 202-209

[11] The statistics Portal. (2014). Types of cybercrime attacks experienced by companies in the United States as of June 2014. Retrieved from http://www.statista.com/statistics/293256/cyber-crime-attacks-experienced-by-us-companies/ on 15 March 2015

[12] Wigder, Z. D. & Bahl, M. (2012). Trends in India's ecommerce Market. *2nd National Conference on eCommerce 2012*

IJMRA