A STUDY ON CYBER SECURITY – ISSUES AND CHALLENGES

Written by ***Jenifer Stella S* & Dr. Ambika Kumari S*****

**Research Scholar, Vel's Institute of Science Technology and Advanced Studies, Chennai, Tamil Nadu, India*

*** Professor and Dean, School of Law, Vels Institute of Science, Technology & Advanced Studies, Chennai, India*

ABSTRACT

Cyberspace is that virtual space in which communication over computer networks occurs. This term became widespread in the 1990s when the uses of the web, networking, and digital communication were all budding radically and the term "cyberspace" was able to represent many fresh ideas and phenomena that were developing. Cyberspace is sometimes also referred as cybernauts. The term cyberspace was introduced for the first time by Norbert Wiener for his revolutionary work in control science and electronic communication. The parent term of cyberspace is "cybernetics", which was derived from the Ancient Greek kybernētēs. As a social practice, individuals can deliver social support, play games, share information, interact with each other , conduct business, exchange their views, involve in political discussion, and so on, using this world-wide network. Cyberspace is a domain categorised by the usage of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures. In effect, cyberspace can be assumed to be the interconnection of human beings through computers and telecommunication, without any regard to physical geography.

Keywords: Cyber Space, Cyber Threat, Cyber Exploitation, Cyber Crime, Cyber Security, Issues, Challenges, Policing & Preventative Strategy.

INTRODUCTION

Millions of people across the globe make use of Internet in day to day activity. The purpose vary, from banking to shopping and to chatting and dating. From a psychological perception, Internet has become a major tool for interpersonal communication that can significantly touch people's decisions, behaviours, attitudes and emotions. Moreover, the existence of cyberspace has created a virtual social atmosphere in which people can meet, convey, work together and exchange goods and information. Cyberspace is not just a technical scheme but a phenomenon which has brought the world to an acquainted global township, nurturing collaborations and international cooperation, thus reducing the blockades of geographical distance and indigenous cultures. Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures.[i] In this effect, cyberspace can be assumed to be the interconnection of human beings through computers and telecommunication, without any regard to physical geography. William Gibson is sometimes credited with inventing or popularizing the term by using it in his novel of 1984, *Neuromancer*.[ii]

On the other hand, cyberspace has proportional demerits with the growing technologies. Cybercrimes are those crimes committed on the Internet, through the Internet and by means of the Internet. Computer crime is a general term that embraces such crimes as phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyberterrorism, creation and/or distribution of viruses, Spam and so on. All such crimes are computer related and facilitated crimes.[iii]Most of the criminals have grown up understanding this information superhighway of , unlike the older generation of users. This is why cybercrimes has now become a nightmare in the United States.

In this digital era, where online communication has become the standard norm, internet users and governments face amplified risks of becoming the targets of cyber-attacks. As cyber criminals continue to develop and advance their techniques, they are also shifting their targets - focusing less on theft of financial information and more on business espionage and accessing government information. To fight fast-spreading cybercrime, governments must team up globally to develop an effective strategy that will help in regulating the threat. Cybercrime, is

any crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Dr. Debarati Halder and Dr. K. Jaishankar define Cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)[iv].

AN INSIGHT INTO CYBER CRIME

Cybercrime is a term for any illegal criminal behaviour that utilizes a personal computer as its essential methods for commission of theft. The U.S. Department of Justice, group's cybercrime into three parts: a computer is the target of an attack, is used as a weapon for an attack or is an accessory to an attack. As we go through the types of cybercrime, we'll let you know in which area they are usually grouped.[v] Further it expands the definition of cybercrime to include any illegal activity that uses a computer for the storage of evidence. The rising list of cybercrimes includes crimes that have been made possible by computers, such as network intrusions and the dissemination of computer viruses, as well as computer-based variations of existing crimes, such as identity theft, stalking, bullying and terrorism which have become as major

problem to people and nations. New developments in technologies make new criminals open doors and gives rise to couple of new kinds of unlawful activity. What distinguishes cybercrime from customary crime? Evidently, one contrast is the use of the advanced Computer, however innovation alone is insufficient for any modification that may exist between various domains of crime. Crooks need not bother with a computer to conduct extortion, traffic in kid sex entertainment and protected innovation, take a character, or damage somebody's security. Every one of those exercises existed before the "digital" prefix ended up omnipresent. Cybercrime, primarily including the Internet, states to an enlargement of existing criminal behaviour close by some novel unauthorised exercises. Mostly cybercrime is an attack on the data of people, organizations, or governments. In spite of the fact that the attack do not take place on a physical body, they do happen on the individual or corporate virtual body, which is the arrangement of instructive properties that distinguish individuals and organizations on the World Wide Web. Eventually at the end, in this computerized age our virtual characters are basic components of our daily being: we are in a mass of numbers and identifiers in different computers databases possessed by governments and partnerships.

Yahoo was the target of one of the largest attacks in cybercrime history. It's confusing how it happened, though. The company announced in September 2016 that it had been the target of an attack in 2014 in which 500 million accounts, including names, email addresses, dates of birth and phone numbers, were compromised. A few months later, it announced that another attack, carried out in 2013 by a different group of hackers, accessed nearly a billion accounts, which included passwords and security question answers. The statement was then revised, revealing that just over 3 billion accounts were compromised. At the time of the announcements; Yahoo was in negotiations with Verizon for sale. After the news broke, an estimated $350 million was taken off the sale price. It's scary to think about, considering it was one of the largest data breaches in history and Yahoo waited three years to say anything about it.

During the same time, or a bit before, the Blackshades RAT was a popular tool for extortion. A RAT, or Remote Access Tool, permits a remote computer to control anybody's computer without any physical connection. Most of the time RATs are used lawfully, such as when a

computer manufacturer provides support. Blackshades, a hacker group, modified a commercially available RAT and used it for extortion. One of the most famous examples was Miss Teen USA Cassidy Wolf in 2014. Her webcam was hijacked and monitored for a year by Jared Abrahams, a classmate who had also cyber attacked 100-150 other women.[vi]

AN OUTLOOK ON CYBER THREAT

Cyber threats are becoming more sophisticated with the blending of once distinct types of attack into more damaging forms.[vii] Increased variety and volume of attacks is inevitable given the desire of financially and criminally-motivated actors to obtain personal and confidential information. Just like many of the battles that we see in the world today, the number of cyber threats has shown growth exponentially in size and scope, from within the boundaries of the firewall to traversing the complete world around the internet. Enterprises in each and every industry and of all sizes are finding themselves under a snowballing barrage of cyber-attacks. Needless to say, the days are gone where a firewall alone was sufficient protection against a cybercriminal or group. The proliferation of connected devices, alongside flexible working practices and complex partner ecosystems have made the boundaries of an organisation ebb and flow. Threat thespians in the cyber space with malevolent intent are taking advantage at an eye-wateringly large cost to businesses.

The elasticity offered by the contemporary business has led to an increased use of third-party suppliers. In fact, a survey from Thomson Reuters entitled 'Third Party Risk: Exposing the Gaps' revealed that 70 per cent of organisations have become more flexible and competitive because of third-party relationships. Although such associations could be beneficial for those involved, but the security threat they pose is often ignored or goes unaddressed. Joining of hands with third-parties and adding organisations to a supply chain in this contemporary world is more dangerous than ever.As these threat actors are now capable to access information preserved by larger organisations through the smaller businesses within the chain, it is no longer enough for enterprises to understand just their own security set up. Such kind of attacks has been shown in recent years by a number of incidents. For example, in 2013, cybercriminals

managed to steal $250,000 from Bangladesh's Sonali bank, along with more than $12million from Ecuador's Banco del Austro in 2015, by using the banks' access to the SWIFT network to send fraudulent messages and transfer money.

As development in the threat scenario is also being identified elsewhere, with a key example being the increasing risk of cyber destruction. Although such form of attack has become prevalent in recent years, it is often problematic for businesses to recognise the reward and the motives behind them. Could it be a student showing off their cyber talents, researchers inventing new methods of infecting a system, or perhaps developers testing their latest malware creations? However, as now there is ample of data accessible which makes them to identify changes in attacker's tactics and defend themselves before they become a target. While it might seem like a luxury, taking the time to stop and think about the actor behind these attacks is vital. Enterprises should start looking at cyber-attacks from the opponent's viewpoint to understand the effects of the attacks and what kind of attacks are more attractive and profitable for the cyber criminals and to know how best to protect against them. Those businesses that are reluctant in understanding the threat which is evolving, glitches will continue and they will fall further behind attackers. Organisations should now start taking action to safeguard their cyber security strategies, and those of the enterprises within their supply chain, are up to date and able to respond to new forms of attacks quickly. Only then they can be safe against the evolving threat landscape.

Ransomware is one of the most aggressive tactics used by today's hackers. These threats take a computer, and sometimes even entire networks, as hostage. Often, all the files and data previously stored on a system become inaccessible until the victim.[viii]

Phishing is intended to induce unsuspecting internet users into downloading annoying applications and providing personal details. Phishing is not just online it can also take place over phone, email, text and more. Phishing can get you in many ways, too. The most commonly used method is to share a malicious link to a user and make them download malware. Such malware could be anything from ransom ware to adware, both of which are covered in our best antivirus software guide. There are other forms of phishing that don't require to click a malicious link, however, such types of phishing are far scarier.

Cyber Stalking can be characterized as the rehashed acts badgering or compromising conduct of the digital criminal towards the unfortunate casualty by utilizing web administrations. Stalking in general terms can be referred to as the repeated demonstrations of badgering focusing on the unfortunate casualty, for example, following the person in question, making bothering telephone calls, murdering the people in question pet, vandalizing exploited people property, leaving composed messages or items. Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously[ix]. Everything relies upon the course of lead of the stalker.

Cyberspace is being extremely used by its abusers to reach and abuse children sexually, worldwide. As internet has become a need of every person every home has access to internet, the more children are addicted to the internet there are more chances of them falling victim to the aggression of paedophiles. The easy access to the pornographic contents readily and freely available over the internet lowers the inhibitions of the children. Paedophiles trap children by distributing pornographic materials, through which they try to meet them for sexual activity and sometimes certain Paedophiles also take their nude pictures as well as their engagement in sexual positions.[x] Paedophiles also try to contact children in the chat rooms posing who are usually teenagers or a child of similar age, they then start their trap by becoming their friend to win their confidence. Gradually they get into sexual conversation to help teenagers shed their inhibitions on sex and then arrange personal meetings. Paedophiles by proposing attractive money or promising them a bright future in life jump into actual misuse of children either by making use of them for sexual purpose or by taking their pornographic photographs to sell them over the internet for a rewarding amount.

Browser hijacking is a cybercrime that is normally utilized for promotion extortion. Malware seizes your program settings, frequently changing the landing page, default web crawler and then some. The new goals show ads that the programmer uses to produce income. While your PC is the objective of program commandeering, promotion extortion falls into the class of utilizing your PC as an extra. Browser hijacking is normal, for the most part in light of the fact that numerous individuals don't realize they are an unfortunate casualty. Robbers are typically packaged with free applications and take on the appearance of an increasingly secure approach to utilize the web. That isn't valid, obviously, and the aggressor utilizes the deception to introduce malware on your machine.

CYBER SECURITY - ISSUES & CHALLENGES

The concept of user name and password has been fundamental way of protecting our Information. This may be one of the first measures regarding cyber security[xi]. For every enterprise and organisations privacy and security of the data are always the top security measures to be taken care of. We are living in a world of cyberspace where each and every data of ours is preserved in a digital form. Social networking sites promises to provide a platform to its users where they feel safe and most importantly an easy going mode of interacting with their friends and family. For home-based users, cyber actors would carry on their target in social media sites to steal personal data and use it for unlawful activities. Such unlawful activities are not limited to social networking sites alone but it is also essential to be careful and take requisite security measures while making bank transactions.

In the present Internet-associated world where innovations support pretty much every aspect of our general public, cyber security and criminological masters are progressively managing wide going digital dangers in practically ongoing conditions. The ability to distinguish, investigate, and safeguard against such dangers in close continuous conditions is beyond the realm of imagination without work of risk insight, enormous information, and AI systems. For instance, when a lot of information is gathered from or created by various security checking arrangements, insightful and cutting edge huge information logical systems are important to mine, translate, and separate learning of these unstructured/organized (enormous) information. Therefore, this offers ascend to digital danger knowledge and scientific arrangements, for example, huge information, man-made consciousness, and AI, to see, reason, learn, and act against digital enemy strategies, systems, and methods. The National Cyber Security Alliance, through SafeOnline.org, recommends a top-down approach to cyber security in which corporate management leads the charge in prioritizing cyber security management across all business practices.[xii] NCSA advises that companies must be prepared to "respond to the inevitable cyber incident, restore normal operations, and ensure that company assets and the company's reputation are protected." NCSA's guidelines for conducting cyber risk assessments focus on three key areas: identifying your organization's "crown jewels," or your most valuable information requiring protection; identifying the threats and risks facing that information; and outlining the damage your organization would incur should that data be lost or wrongfully exposed[xiii].

Cyber security has turned into the present stage for current fighting. It has enabled countries to lead data fighting which has modified the race results to specifically assaulting a country's capacity web for developing nations, this should raise alerts and fill in as a reminder to set up solid cyber security arrangements that move toward becoming established in training, innovation, and laws. With about 30 Million sightseers travel to the Caribbean and spending upwards of $35 billion out of 2016 this territory fills in as a practical objective for assaults roughly 25 % of those explorers go to the Dominican Republic. These sightseers go to the island ignorant of the cyber security challenges confronted and the developing worries inside the nation. It is realized that regarding security, a system will be as solid as its weakest connection. This saying can be connected to the circumstance of cyber security of the nations

of the Central American Region (CAR), from the specific situation and the truth of a hyper connected world. The absence of data security culture is one of the fundamental hindrances when endeavouring to actualize a national IT security strategy.

CONCLUSION

With the spread of PCs and web, digital wrongdoing has developed as a noteworthy test for law authorization organizations. The web conveys satisfaction to our lives and yet it has some negative sides as well. The digital hoodlums are continuously in an inquiry to discover the better approaches to assault the conceivable web unfortunate casualties. Today, everyone is utilizing the PCs for example from white neckline representatives to psychological oppressors and from young people to grown-ups. The more youthful ages, which use the web and other online advancements widely for remaining associated for the entire day to day work and excitement, including data, messages, interpersonal interaction, e-banking, e-shopping, web-TV, news, instruction, home-work look into, internet gaming, downloading music, recordings, motion pictures and other substance and so forth, are progressively helpless against focused digital wrongdoing. All the ordinary wrongdoings like falsification, blackmail, capturing and so on are being finished with the assistance of PCs. In this way the the internet can be utilized either lawfully or illicitly. In this way it is on one's hand to utilize it adequately.

Many data breaches result from phishing scams that introduce malware into network systems.[xiv] Educating people regarding the latest tactics used by scammers can help reduce the likelihood that they will click links that expose them to malicious software. Implementing basic data security policies that explain how to properly handle personal and official data is also key to reducing the threat of internal misuse. Organizations should also be stricter about who has access to sensitive data in the first place. These strategies can greatly reduce the impact of human error on cyber security measures. While cyber-attacks remain a serious threat to organizations today, there are several solutions that can bolster efforts to safeguard data and maximize service uptime. By keeping up-to-date with the latest risks, we can implement more effective cyber security strategies to protect ourselves from harmful data breaches and other threats.

REFERENCES

1. Z Kotulski, T.W Nowak, M Sepczuk, M Tunia, R Artych, K Bocianiak, T Osko and J-P Wary (2018). Towards constructive approach to end-to-end slice isolation in 5G networks. *EURASIP Journal on Information Security, 2018,* 2, Published on: 20 March 2018 https://doi.org/10.1186/s13635-018-0072-0.
2. B. Young, "A study on the effect of Internet use and social capital on the academic performance", "Journal of Development and Society", vol. 35(1) pp. 107-123, 2006.
3. F Sharevski (2018). Towards 5G cellular network forensics. *Eurasip Journal on Information Security, 2018,* 8, Published on: 11 July 2018 https://doi.org/10.1186/s13635-018-0078-7.
4. T. Makasiranonth, "Internet addicting behavior and factors related to internet addiction", Master degree, Chulalongkorn University, Bangkok, Thailand, 2002.
5. P Parrend, J Navarro, F Guigou, A Deruyver and P Collet (2018). Foundations and applications of artificial intelligence for zero-day and multi-step attack detection. *EURASIP Journal on Information Security 2018,*4, Published on: 24 April 2018 https://doi.org/10.1186/s13635-018-0074-y.
6. A Sitek and Z Kotulski (2018). POS-originated transaction traces as a source of contextual information for risk management systems in EFT transactions. *EURASIP Journal on Information Security 2018*,5, Published on: 27 April 2018 https://doi.org/10.1186/s13635-018-0076-9.
7. S.M. Li, and T.M. Chung, "Internet function and Internet addictive behavior", "Computers in Human Behavior", vol. 22(6), pp. 1067-107, 2006.
8. J Navarro, V Legrand, A Deruyver and P Parrend (2018). OMMA: open architecture for operator-guided monitoring of multi-step attacks. *Eurasip Journal on Information Security, 2018,*6. Published on: 2 May 2018 https://doi.org/10.1186/s13635-018-0075-x.
9. J.H. Jeon, "The effect of extent of Internet use and social supports for adolescent depression and self-esteem", unpublished master's thesis, Seoul: The Graduate School of Yonsei University, 2005.

10. G Jaideep and B.P Battula (2018). Detection of spoofed and non-spoofed DDoS attacks and discriminating them from flash crowds. *Eurasip Journal on Information Security, 2018*:9. Published on: 16 July 2018 https://doi.org/10.1186/s13635-018-0079-6.

ENDNOTES

[i] Edited by Leslie W. Kennedy, Edmund F. Mc Garrell (2011)Crime and Terrorism Risk: Studies in Criminology and Criminal Justice
[ii] https://whatis.techtarget.com/definition/cyberspace
[iii] https://cyberlawsindia.net/internet-crime.html
[iv] https://www.ccfanigeria.org/what-is-cyber-crime/
[v] https://www.cloudwards.net/cybercrime/
[vi] https://www.cloudwards.net/cybercrime/

[vii] https://www.sciencedirect.com/science/article/pii/S0167404811001040

[viii] Cybercrime: The Complete Guide to All Things Criminal on the Web/By **Jacob Roach** – Deputy Editor
[ix] https://www.iracst.org/ijrmt/papers/vol6no12016/2vol6no1.pdf
[x] http://crimebranchjkpolice.nic.in/cybercrime.html
[xi]https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies

[xii] https://digitalguardian.com/blog/what-cyber-security
[xiii] https://digitalguardian.com/blog/what-cyber-security
[xiv] https://www.vxchnge.com/blog/cybersecurity-problems-and-solutions