Impact Factor : 1.883 Peer-Reviewed Journal ISSN : 2278 – 5639
Global Online Electronic International Interdisciplinary Research Journal (GOEIIRJ)
{Bi-Monthly} Volume – IV, Issue – II August 2015

CYBER SPACE – WHAT SHOULDONE KNOW ABOUT IT ?

Dr. Anita Chaware

Abstract

In the modern world, which is controlled almost entirely by technology and network connections, it is very necessary to be familiar with the concept of cyber space. Cyber space has become very valuable and heavily used resource in the Universe. If there is no security to secure it, then the your essential files, data, and other important virtual items on your computer are at danger. Not only this you identity become unsafe. Every individual / organization, regardless of whether it is an IT firm or not, needs to be safeguarded in the cyber space. This paper explains in brief Cyber space or commonly known internet. It also discuss the different components, threats and precautions to be take while working on the cyber space. This paper bring the IT law acts amendment to the notice of the readers.

Introduction

The concept cyberspace is a modern origination from the science fiction writer William Gibson, who used the word for the first time in his book "neuromancer" published in 1984. The word has now become a conventional way to explain anything related to computers , information technology, the Internet and the varied internet culture. Cyberspace, as Gibson describes it, is now a network space connecting digital data stores which can be accessed and interacted with via a computer connected to the network. Such spaces called as "Internet" are a vast collection of computers linked to networks within larger networks spanning the globe. Anyone with a computer, a modem and a telephone can connect to each other through- out the globe via Internet. In this cyberspace there are cyber societies communities which communicate with friends, search for information, do banking transactions, availing online services, finding job, finding life partner or even run entire businesses. The internet touches almost all aspects of our lives. However, it also makes us vulnerable to a wide range of threats.It offers users a range of interactions, allowing them to explore the world beyond their personal computer or home computer. Its very easy to peep into others world via internet in the cyberspace. Users can browse information stored on other computers, exchange electronic mail, participate in discussion groups on a variety of topics, transfer files, search databases, take part in real-time conferences and games, and run software in the cyberspace..

Thus, cyberspace is the electronic and telecommunication universe formed and maintained

by the world's computers and communication lines. It is an atmosphere in which global knowledge, mysteries, dimensions, pointers, showbiz and other human beings take the form that never flourished on the Earth's surface.

Mathematically, Cyberspace = networking(ICT) + visualization(virtual space) , Cyberspace is composed of a networking and a visualization part.

To summarize, Cyberspace, created by communication technologies especially the Internet, is a virtual space where people can access, interact and communicate through physical devices independent of time and space. It is a digital space and has no actual physical location. Therefore, people can easily communicate in cyberspace regardless of the limitation of geographical distance. Due to its convenience, cyberspace has been widely applied in people's daily life and it gradually becomes an indispensable space, paralleled to geographic space.

Statistically, In 2020, India had nearly 700 million internet users across the country. This figure was projected to grow to over 974 million users by 2025, indicating a big market potential in internet services for the south Asian country. In fact, India was ranked as the second largest online market worldwide in 2019, coming second only to China. The number of internet users was estimated to increase in both urban as well as rural regions, indicating a dynamic growth in access to internet.

Different Components of Cyberspace—Physical Systems, Information, Cognitive Actions, and People

Cyberspace is a man-made Ecosystem. Cyberspace needs the human being activities and attendance. Cyberspace fuses all the global virtual infrastructure comprises ICT networks, databases and knowledge sources. Cyberspatial Economy, politics, armed systems include Strengths, knowledge and psychology

The basic physical components of cyberspace are the physical devices / systems which create It. Cyberspace is a connected virtual space made up of physical systems or devices like computers and servers, supercomputers and grids, sensors, transducers, and the Internet as well as other supporting networks and communications links.

Data is the new Gold. Each click, like, and share creates new data in the world,Creating, recording, storing and processing the information is center of cyberspace . Information in Cyberspace takes several forms like text, posted music and Images, stored company documents, and all www Pages all over the Internet along with tons of data generated dynamically at every click on the internet. .

The main objective of the cyberspace is cognitive actions like the manipulation of

information to change thoughts and behaviors.

People are as important a component of cyberspace (or more so), than are wires and protocols. Technically, cyberspace generally describes an interface between computers and people, or a meeting point for digital information and human perception.

Some researchers also provide societal and cyberspace infrastructure. The Internet, however, is the fundamental part of this modern world.

Cyber space is only a concept which is further refers to the word Digitalization. It produces huge amounts of data, if used efficiently, offer opportunities for business, human well-being and the environment. much of information can be used to deliver relevant marketing information and bring increased value to consumer audiences thus created threats in cyberspace called cyber-attacks. Our societal , economical and critical infrastructure have largely become digitalized. As our dependence on information technology grows, cyber attacks become more appealing, and potentially more destructive.

Existing and emerging Threats in Cyber space– the Cyber attacks

Cyber-attacksare quicker, more comfortable and less dangerous than physical ones for the attacker. Just a few expenses beyond a computer and Internet connection are required for cyber criminals. Geographical distances are unrestricted. Owing to the anonymous existence of the Internet, they are difficult to track and prosecute. Since attacks on information technology systems are very attractive, the number and complexity of cyber-attacks is expected to continue to increase.

Malware refers to a wide variety of attacks loaded on a system to compromise a system for an adversary, normally without the knowledge of the system owner. Malware examples include, viruses, worms , Trojan horses, Phishing , Cross-Site Scripting, Ransomware, spyware, adware, keylogger, and bot /botnets/bot executable[15]. Cyber criminals/ hackers / malicious actors/ cyber attackers whatever you call them, design malicious software's for compromising computer processes, stolen data, bypass access controls and damage the host computer, servers and the networks applications or data otherwise. The oldest virus was thought by the father of computer as a self-replicating computer programs in 1949, actually appeared in the '70s The majority of cyber attacks today still occur as a result of exploiting software vulnerabilities caused by software bug and design flaws [104]. The different categorigies of Cyber attcksas Identity Theft : When someone takes your personal information, such as your Social Security Number, bank account number, and credit card information, this is known as identity theft.

Psychological attacks : The term "psychological abuse" refers to the repeated and deliberate use of a broad diversity of words and actions that do not involve physical contact and are with the intention of

controlling, hurting, weakening, or frightening a person on a mental and emotional level; and/or distorting, confusing, or otherwise influencing a person's thoughts and actions.

Social Media related Attacks : Facebook, Snapchat, and Instagram are the most visited social media through which the attackers or Cybercriminals create fake accounts, Compromised Profile, malicious links to lure a victim into clicking through to a data that is hosted on third-party sites which can be very damaging to the individual or the organization as whole.

Virus Attacks onPersonal Computer: A computer virus is a type of malicious software that is attached to another programme (such a document) and has the ability to multiply and propagate after being executed on a computer for the first time by a user. For instance, you may get an email with a harmful attachment, open the file without realizing it, and then find that your machine is infected with a virus. This virus will either corrupt your data or information without your knowledge.

Digital BankingFrauds: with more and more digitalization in banking and financial sectors there will be many digital banking frauds. Hacker will hack the systems and transfer a huge amount through internet.

What is the impact of cybercrime ?

Crimes committed online are not limited by national boundaries and keep pace with rapidly advancing technology. The expenses that are connected with cybercrime are enormous for both individuals and businesses. Theft of intellectual property, theft of personal and financial data, post-attack disruption to the normal course of business, reputational harm, and more are some of the costs associated with cybercrime. Other costs include loss of data and degradation of data, stolen money, lost efficiency, theft of money, theft of personal and financial data, and more. The inability to safeguard their intellectual property (IP), financial information, and information technology (IT) networks does, in fact, have an economic impact, as well as a cost associated with their reputation, and a cost associated with the regulatory requirements.

Economic costs : Theft of intellectual property, corporate information, disruption in trading and the cost of repairing damaged systems

Reputational costs: Loss of consumer trust, loss of current and future customers to competitors and poor media coverage and liability risk for the affected company and its brand

Regulatory costs: GDPR and other data breach laws mean that your organization could suffer from regulatory fines or sanctions as a result of cybercrimes

Nappo in his article has said "Cyber-Security is much more than a matter of IT. It takes 20

years to build a reputation in business and few minutes of cyber-incident to ruin it."

Safety measures on Cyberspace/Internet

Keep Personal Information on the internet / cyberspace Professional and Limited.

Create nicknames that do not reflect your own name or anything personal.

Never give your password to anyone. Your banks will never, ever ask you for your password while you are online or via email.

Keep Backups of Important Files and Folders fromyour computer.

Don't provide your credit card number and date of birth to anybody on phone or do not enter these important data on any website or do not give personal information to someone unknown to you.

Use strong passwords. Every time creating a new password read the instruction give on website.

Be careful while downloading any attachment rom the email or downloading ay free software or screensaver etc.

Never meet face-to-face with someone who is just your internet friend.

Check the website name carefully.

Always LOGOUT or SIGNOUT

What does cyber law says in case of some cybercrime

The word "cyber law," which is also spelled "cyber-law," is a term that is used to define the legal difficulties that are associated to the usage of communications technology, namely "cyberspace," which refers to the Internet. Robbers no longer carry firearms; instead, they utilize a computer mouse, a cursor, and passwords to do their crimes. Awareness campaigns and following best practices in cyber security are two ways to lessen the impact of these risks Currently few things more has added into this law. The **Information Technology Act, 2000** IT act is given by Indian govt for cybercrimes.

Information Technology (Amendment) Act, 2008

- **Voyeurism** is now specifically covered. Acts like hiding cameras in changing rooms, hotel rooms etc is punishable with jail upto 3 years. This would apply to cases like the infamous Pune spycam incident where a 58-year old man was arrested for installing spy cameras in his house to 'snoop' on his young lady tenants.
- Publishing **sexually explicit acts** in the electronic form is punishable with jail upto 3 years. This

would apply to cases like the Delhi MMS scandal where a video of a young couple having sex was spread through cell phones around the country.

- Collecting, browsing, downloading etc of **child pornography** is punishable with jail upto 5 years for the first conviction. For a subsequent conviction, the jail term can extend to 7 years. A fine of uptoRs 10 lakh can also be levied.
- The punishment for a **obscene material** by email, websites, sms has been reduced from 5 years jail to 3 years jail. This covers acts like sending 'dirty' jokes and pictures by email or sms.
- **Compensation** on cyber crimes like spreading viruses, copying data, unauthorised access, denial of service etc is not restricted to Rs 1 crore anymore. The Adjudicating Officers will have jurisdiction for cases where the claim is uptoRs. 5 crore. Above that the case will need to be filed before the civil courts.
- A special liability has been imposed on call centers, BPOs, banks and others who hold or handle **sensitive personal data**. If they are negligent in "implementing and maintaining reasonable security practices and procedures", they will be liable to pay compensation
- Refusing to hand over passwords to an authorized official could land a person in prison for upto 7 years.
- The offence of **cyber terrorism** has been specially included in the law. A cyber terrorist can be punished with life imprisonment.
- Sending **threatening** emails and sms are punishable with jail upto 3 years.
- Hacking into a **Government computer or website**, or even trying to do so in punishable with imprisonment upto 10 years.
- Cyber crime cases can now be investigated by **Inspector** rank police officers. Earlier such offences could not be investigated by an officer below the rank of a deputy superintendent of police

Conclusion :

Because practically every person in the world now has a basic understanding of technology, we are now having to deal with a rise in the number of crimes that are associated with technology and are referred to as cybercrimes. The ever-increasing number of cyber security risks is putting a strain on organisations, who are finding themselves in the position of having to respond to them. Even while not everyone becomes a victim of cybercrime, that does not mean that they are not at danger of being a victim. Lack of awareness and lack of security may lead to data loss, information loss, financial loss, and other types of loss, as we have stated before in this article that individuals should be introduced to cyber security from a very early stage in life, so that there would be minimal possibilities of getting stolen. Cyber security enables us to better protect our networks, information, operations, applications, and other critical infrastructure. The actions of workers inside an organisation are a significant factor in the formation's overall level of safety.

References :

1. Amoroso, E. 2006. Cyber Security. New Jersey: Silicon Press.
2. Baldwin, D. A. 1997. The Concept of Security. Review of International Studies, 23(1): 5-26
3. https://eprocure.gov.in › cppp › rulesandprocs
4. https://www.itlaw.in/
5. "computer security | Definition & Facts | Britannica", retrivedfrom . www.britannica.com