Vidya Journal of Engineering & Technology
ISSN 2277-8978, Vol. 3, No. 1, Jan-Dec 2017, pp. 48-54

CYBER SECURITY: A NEED IN GLOBALIZATION

Prakhar Agarwal, Neetu Bansla* & Shivani Jain**

ABSTRACT

Today's world is on verge of high technology equipped communication in lieu of the need for globalization. These approaches emphasize on high speed communication and elaborated modes of data transfer throughout the world. These approaches mainly endeavor high competition between the trading and fastest spreading of any kind of information. In order to fulfill the mentioned reasons, the wholesome communication is desired to be online i.e. with of help of internet. As the world goes online, a security threat comes into the mind. Threat is something that one does not want to but it happens undesirably. Moreover, a threat is due to a heavenly loss of some crucial or precious thing. Here by the word "Threat" we mean – threat to our critical data, confidential information, sensitive details, personal stuff, personal information etc. Today, irony is this; we cannot live in isolation i.e. by not sharing any data online or by not at all visiting the internet. And communicating on internet means putting your data, information, details etc. on verge of getting disrupted corrupted, leaked, accessed by unauthorized person or completely lost. Therefore, to overcome or to minimize the mentioned losses, a security measure is needed which gives either a protection or assurance that the data will be safe or retrieved if gets disrupted; Communication will be secured through the internet. Such a security measure is often termed as "Cyber Security". Cyber security means related to the internet. Cyber security enlists a number of cyber laws to go hand in hand with cyber security. We in this paper try to brief the definition, problems, importance and some real life scenarios related to cyber security.

Keywords: *Cyber security, Threat, Globalization*

* Vidya College of Engineering, Meerut

I. INTRODUCTION

In today's globalized, techno-savy world of highly renewed technologies where each and every corner of information transfer is being governed on internet world wide that is being communicated through internet, also known as online transaction. As technology brings in a lot of effort less jobs, it poses a threat to our confidential data by means of different malicious activities such as – hacking, eves dropping, denial of service, fishing, middleman attack etc. The term cyber security is often used interchangeably with the term information security. Cyber security has become crucial on top of the harsh and turbulent business environment. The internet has been recently changed into a minefield for digital crime, information leakage, cyber harassment, and cyber-attack on a large scale [1].

In order to protect our data from such attacks we need some security measures which will help in overcoming big losses and such type of security is known as cyber security. Several examples can be cited for describing the theft of crucial data such as :

1. Social Media frequently asking for giving access to personal detail – most of the times people being ignorant never denies to these activities.
2. Frequent sharing of data on social media through mobile phone-sometimes fake profiles may appear using one's personal information.

Therefore, in order to protect our data or to retrieve our data we have certain laws governing the same known as cyber laws. Looking minutely at the reasons of cyber attacks- one of the aspect is the internet. Whenever a system is connected via internet it more vulnerable to attacks and the consequences can be very harmful such as hacking of a personal computer thereby a taking hold of all the data in the system. Person involved in such activities can arise in groups in pair of two or even as an individual and hence can be termed as cyber criminals. They detroit one's image socially by posting any personal or offensive stuff online which is quite a heinous act.

Globalization demands a lot of involvement of communication via internet, on-line transactions covers a lot of part of the same. Rising demands and need of reaching overseas compel an individual to cover the whole world and internet helps in achieving the same. But technology always brings in a lot of curse simultaneously being proved as a boon. Therefore, in order to carry the daily tasks while taking help of technology, a digital security is needed to protect the crucial data.

II. TYPES OF CYBER SECURITY ATTACKS

One of the biggest security problems is perception: The threats companies think they face are often vastly different than the threats that pose the greatest risk. For example, they hire me to deploy state-of-the-art public key infrastructure (PKI) or an enterprise-wide intrusion detection system when really what they need is better patching. The main thing is that companies face the same threats and should be doing their utmost to counteract those risks [2].

The most common types of attacks could be considered based on reports from the Ponemon Institute [3].

(a) Virus Attacks-Attacking through malwares such as Trojan horse, worms etc.

(b) Phishing Attack-where a third party trust is involved which steals the information by faking the identity.

(c) Brute Force Attack-Password attacks such as brute force attacks which uses several methods to break the password.

(d) Denial of service attacks-where a large volume of data is sent to the user thereby blocking all the functions.

III. IMPORTANCE OF CYBER SECURITY

(a) Reduce potential losses due to security attacks such as data loss, bad usage of computer resources, reputation loss.

(b) To secure crucial data like passwords and any kind of encrypted detail used in daily on-line transactions.

(c) To secure day to day transactions this involves personal details.

(d) To reduce chances of distorting information used for critical operations as in today's scenario most of the work is done through internet due to unavailability of persons within nearby vicinity or spreading of work overseas thereby increasing the scope of work.

(e) Cyberspace is becoming a dangerous place for all organizations and individuals to protect their sensitive data or reputation. This is because of the numerous people accessing it.

(f) There is always a game between cyber attackers and offenders. These games have high stakes, difficult decisions and short timescale. Most researchers in this area have focused on the strategic level decisions. This focus emphasis on the origin of the game. This approach however lacks flexibility once a high level is reached. This situation is often compared to a turn-based style of play where we hope to end the game quickly, for example, by obstructing the execution of a software program when a signature is detected that matches some definition of malicious stuff [4].

One important indicator is the IT skills of a person that wants to hack or to invade the security. This is because of three main factors:

(a) Easily found hacking tools that are available just by googling and they are endless.

(b) Increased technology over the years such as speed of processing increased bandwidth etc.

(c) Availability of hacking manuals.

IV. WHAT TO SECURE?

(a) Check the physical security by setting control systems like motion alarms, door accessing systems, humidity sensors, and temperature sensors. All these components decrease the possibility of a computer to be stolen or damaged by humans and environment.

(b) An individual must have his/her own user id with password protection.

(c) Network should be secured especially wireless.

(d) Routers should be protected with passwords.

(e) Data encryption should be done.

(f) Data Transmission & modes should be protected.

V. METHODS

Cyber Security Research Methods teaches scientific methods for creating knowledge, proven theories, and adding important rigor to the cyber security field [5].

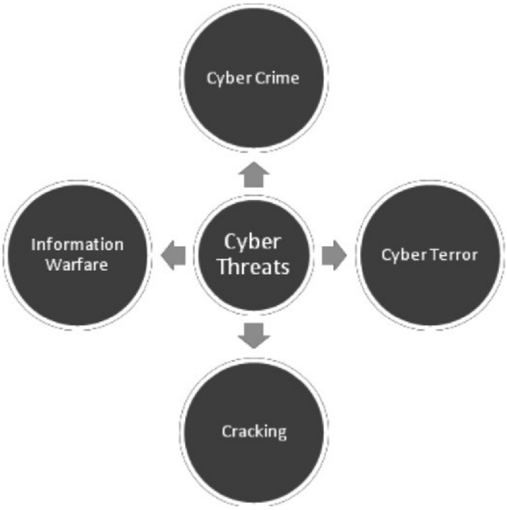

Fig. 1 Methods of Cyber Security

1. Different Elements in Cyber Security

(a) Confidentiality-It is the concealment of information or resources while communicating the information.

(b) Integrity-It has to do with the content of the data and authentication which has to do with the origin of the data as such information has values only if it is correct.

(c) Availability-The ability to access data of a resource when it is needed.

2. Layer Architecture In Cyber Security

(a) Computer Application White listening for installing just stricter number of applications in computers.

(b) Computer System Restore Solution to retrieve the lost files again.

(c) Computer and Network Authentication for authorized access over the network.

(d) Remote Access Authentication to prevent any unauthorized user who is listening to the network distantly.

(e) Network Folder Encryption for it is good to be encrypted to prevent any unauthorized user.

VI. BASIC FUNCTIONS OF ANTIVIRUS CYBER SECURITY

(a) Antivirus producers start writing programs that that scans for similar signature strings when a new virus is detected and is known as scanning.

(b) Checking for manipulated files in OS from the viruses known as integrity checking.

(c) Checking for Trojans and checking requests made by the operating system for network access.

VII. ENCRYPTION IN CYBER SECURITY

It is a transformed type of genuine information where only the authorized parties know how to read it. The bases of encryption are since the ancient times. A good example is the pigeon couriers, but when the enemies caught them, they could not read them just that the message was lost. Here the encryption is for good or bad purpose. The bad case is the scenarios in which most of the malware files are in an encrypted form, so it cannot be read by everyone accept the hacker.

Cyber Security Encryption Tools

(a) **Axcrypy-** Open source encryption files software.

(b) **GnuPG-**It can be integrated with other software and is also an open source.

(c) **Windows BitLocker-**It is an integrated tool and its main function is to secure and encrypt all the hard disk volumes.

(d) **File Vault-**It secures as well as encrypts all the hard disk volume.

VIII. DATA BACKUP

The main purpose is to recover the lost data from an unpredictable event like deletion by mistake or file corruption which in many cases is caused by a virus. An example is Ransom ware, which encrypts all the data when the computer gets infected and the second is to roll back the data at a specific time. Some back up devices are-CD and DVD, Blue-Rays, Removable Devices such as removable USB or external hard disks, network attached storage (NAS), storage area network (SAN).

IX. TYPES OF BACKUPS BASED ON LOCATION

The types of backup can vary on the size of the business, budget and the data importance.

They are divided in two types-

(a) Local Backups-stored in CD, NA storages

(b) Online Backups

X. CONCLUSION

Even large organizations with top talent and significant resources devoted to cyber security have suffered major cyber security compromises and organizations that do not have such levels of latent or resources face even greater challenges. All organizations need to understand their threat environment and the risks they face, address their cyber security problems, and hire the most appropriate approaches and people. Although the need for cyber security workers is likely to continue to be high, it is difficult to forecast with certainty the number of workers required or the needed mix of cyber security knowledge and skills. Moreover, there are several factors that may affect future need. These include –evolution of cyber security challenge as technology, advances-such as better quality, more secure software, more productive cyber security tools, and better training change with the advent of technology, responsibility for cyber security and shift from organization at large to more specialize information technology or cyber security firms which may reduce the number or change the mix of cyber security workers needed.

REFERENCES

[1] **Farzan Kolini and Lech Janczewski,** (2017), “Clustering and Topic Modelling: A New Approach for Analysis of National Cybersecurity Strategies”, PACIS Proceedings, pp. 1-12.

[2] **Roger A.Grimes,** Security Advisor, https://www.csoonline.com/article/2616316/data-protection/security-the-5-cyber-attacks-yo u-re-most-likely-to-face.html.

[3] **Mehrnaz Akbari Roumani, Chun Che Fung,** (2016), “Value Analysis of Cyber Security Based on Attack Types”, Information Technology Management Society, ITMSOC Transactions on Innovation & Business Engineering, Vol. 1, pp. 34-39.

[4] **Robert Mitchell and Andrew Fisher,** (2017), “Linkography ontology refinement and cyber security”, Computing and Communication Workshop and Conference (CCWC), IEEE, Vol. 3, pp. 67-71.

[5] **Thomas Edgae and David Manz,** “Research Methods for Cyber Security”, ISBN: 978-0-12-805349-2.