Cyber Security Need of Digital Era: A Review

V. L. Badadare
Department of Comp Sci,
Vivekanand College,
Kolhapur (MS) India

R. Y. Patil
Department of Comp Sci,
Vivekanand College,
Kolhapur (MS) India

V. B. Waghmare
Department of Comp Sci,
Vivekanand College,
Kolhapur (MS) India

ABSTRACT

In this Digital era, we are breathing inside the Cyberspace. Cyberspace is the “Virtual computer world” or one can say it as “Internet Connected System”. In India, we are approaching the modernization, globalization to turn into a smart city. To seek the stimulating ambiance in this smart city we have to depend upon Cyberspace where our private information is becoming more vulnerable, which face up to cyber attacks. The Smartphone era provoked the scene where hackers have more space to attack and destroy the cyber world. On the ground of social media network, people are allowed to share their thinking, emotions, status of life without any restriction which leads to a handshaking condition for hackers. If Cyber security policies are properly executed, it will immobilize cyber threats.

General Terms

Network, Cyber Security.

Keywords

Cyber, Cyber Security, Cyberspace, Cyber attacks, Risk Management.

1. INTRODUCTION

In the sphere of Information Technology, The Internet is a milestone for sharing information. A gigantic part of the internet is represented by social networks. This is an effective media for communicating with family and friends. Geographically scattered people keep in contact with this virtual and economical tool. Dependence on this virtual sphere is increasing day by day.

The thriving reliance on Cyberspace has confronted severe Cybercrime. Cyberspace is not a static sphere, but rather a swift, flexible, prevalent sphere subject to open borders and one-sided attacks. Cyber Security as the name suggests, it is a protection of Cyberspace (Internet-connected system). It includes security or protection of hardware, software, and data. Cyber security contains some rigid practices that are designed to protect systems, networks and data from cyber attacks. Effective cyber security diminishes the peril of cyber threat and gives protection to users from the illegitimate exploitation.

Cyber attacks can propel serious damage to your smart devices, online services at a personal level while firms, companies suffer from noticeable financial and reputational damage after receiving cyber attacks. Not only Number of cyber threats is increasing day by day, but the severity of these threats is to skyrocket. Numerous forms of cyber catastrophe have reached a level of overriding the competency of most organizations to battle against. The elevation of cyber threats has increased enormously in the recent years. Most of the cyber attacks are related to recent and past events in the social, political, economic, and cultural magnitudes in the human cosmos.Today, Cyber attacks are managed by thug teams and breach agencies. Now hacking and cracking is not just a hobby; as hackers are getting ample funding it has become a profession. To mollify the stuff of these cyber attacks we should make our Cyber security sturdier. A rigid Cyber security base will provide organizations the confidence to build the blueprint of Cyber security [1, 2].

2. GOALS OF CYBER SECURITY

All The Primary goal of Cyber security is to protect the cyberspace asset. In the context of cyberspace, the term “Asset” refers to any organizational or personal resources that are going to face cyber attacks and which then requires protection from cyber threats. Cyberspace assets include a variety of resources such as hardware (physical computer system), software, networks, data resources, utilities etc.; it may include less tactile resources such as reputation, esteem.

These cyberspace assets have some security necessities such as confidentiality, integrity, availability.

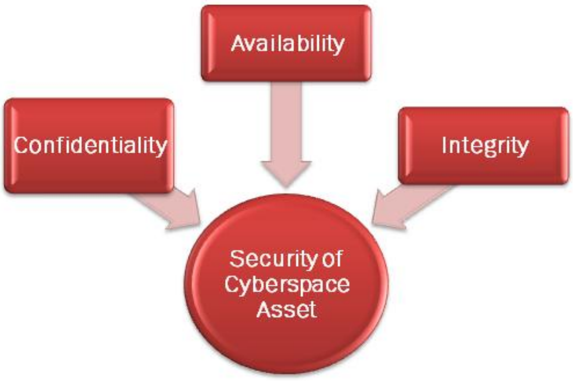

Fig 1: Goals of Cyber Security

2.1 Confidentiality

The term Confidentiality of cyberspace assets regards to stuffing of cyberspace asset is known to only authorize owner. Confidentiality may be achieved by implementing data encryption. This encryption can be of single file, database, disk etc. depending upon type and volume of data.

2.2 Integrity

Integrity of cyberspace asset may unfavorably impress by unauthorized alteration for example, database information may be altered by deliberate unauthorized attack or any accidental extortion. Compromise with system integrity leads harm to information and non-information asset both.

2.3 Availability

Availability to Cyberspace asset means competence to keep trustworthy and prompt access to authorized individuals [3].

3. TYPES OF CYBER ATTACK

With compelling advancement of elevation of IOT (Internet of Things), the Cyberspace security appeal is increasing.

Cyberspace is frequently exposed to various types of attacks which can cause diverse catastrophe. It ranges from meager to major risk

To battle with cyber attacks, we must know about the nature of risks propagated by cyber attacks. Some of the various types of cyber attacks are as below:

3.1 Malware Attacks

Malware is defined as, It is a malicious code targeted to steal, alter or destroy the data in the system. Malware includes various kinds of viruses, spyware, worms, trojans etc. Malwares are automatically spread out by attaching mails, software downloads and software vulnerability.

Malware attack is prevented by some of the following ways:

- Using updated antivirus and Anti-spywares
- Deploying latest and sturdy firewalls
- Avoid attaching unknown mails

3.2 Password Attacks

Password is generally used as identification of the user at the time of authentication process. Obtaining any password unofficially is the emphatic way of Password attack.
Password attack is prevented by some of the following ways:

- Don’t share your password/passwords with anyone.
- Make your password strong so that no one can handily crack your password
- Change your password intermittently.
- Don’t save your password on any website.
- Make sure that you are on official website at the time of entering your password.

3.3 Denial of Service Attack (DoS Attack)

DoS attack is a type of cyber attack where attackers have a mind to make resources unavailable to its expected users. It is done by flooding the network or resources by surplus requests. Purpose of DoS attack is not to harm or steal data of any system but to interrupt the online services.

3.4 Phishing

In phishing attack, we seem that incoming emails are from trusted sources which in consequence take us to some unauthorized site. The central target of phishing attacks is to gain personal information of users; it also influences the users to do something. It could involve processing of malware downloading when we click on the link.

3.5 Man in the Middle (MITM)

Man in The Middle attack is a type of cyber threat where an attacker places himself between the client-server communications. Hackers secretly alter the trusted client-server communication. Some Common examples of MITM are IP spoofing, session hijacking, Replay etc.

3.6 Drive By Downloads

In drive by downloads attack unexpected softwares are downloaded automatically. It is prevalent practice to spread viruses, malwares, spywares etc. Drive by downloads may takes place at the time of fetching unknown email attachments, visiting unauthorized websites, clicking on links.

3.7 Malvertising

Malvertising as the name identifies, It is the “Malicious advertisement”. It works by infusing online advertisement for the purpose of spreading malware to authorized websites or web pages. As the attractive online advertisement influences the users, it’s the sound podium for spreading viruses, malwares, spywares etc[4,5,6].

4. RISK ASSESSMENT

To make the Cyber security system rigid, one should assess the possible risks of Cyberspace.

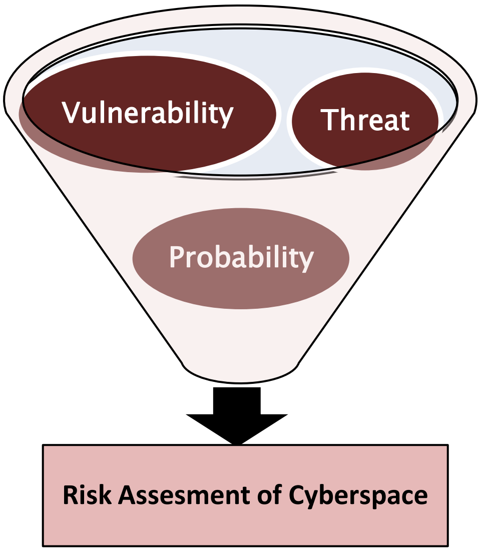

Fig 2: Risk Assessment of Cyberspace

4.1 Threat

Threats to the Cyberspace might be from variety of sources like those springing from people and those springing from elsewhere

4.1.1 Threats originating from people

Assorted people create hazardous condition for Cyberspace considered as threat sources for Cyberspace. Precise list of people treated as threat sources is as below:

- Employees
- Customers
- Vendors
- Former Employees
- Black-hat hackers

4.1.2 Threats originating from elsewhere

Non-People sources creating threat for cyberspace may be some environmental conditions such as adverse weather, temperature etc.

4.2 Vulnerability

Vulnerability means Proneness to protection of Cyberspace asset. Vulnerability is one of the perils for cyberspace protection which can negatively impact the cyber security requirements (Confidentiality, Integrity, and Availability).

4.3 Probability

Probability of risk for cyber security is occurrence of particular risk in the cyberspace. This probability of cyberspace risk may be categorized as “High”, “Medium”, “Low”. Assessment of risk probability allows focusing on particular cyberspace risk, which in consequence improves the cyber security posture [7].

5. CYBERSPACE RISK MANAGEMENT

Peril to Cyber security can be managed by various ways as below:

5.1 Cyberspace Risk Acceptance

Cyberspace risk may be accepted or one can say Cyberspace risk is acceptable when the level of risk is aligned with organization’s policies and standards.

5.2 Cyberspace Risk Avoidance

To genuinely avoid the Cyberspace risk, one has to pretend like simply no risk has arised. The Cyberspace risk is avoided when the associated risk was considered to be too lofty.

5.3 Cyberspace Risk Treatment/Mitigation

Cyberspace Risk Treatment (Mitigation) is a vital aspect in Cyber Security System. Mitigation or Treatment of risk in Cyberspace focuses on two faces:

I. Reducing the probability of Cyberspace risk
II. Reducing impacts of risk on Cyberspace

5.4 Cyberspace Risk Insurance

Today Cyberspace risk insurance has become a trendy affair. It is considered as the highly anticipated redress for high-impact Cyber security risks. Cyberspace insurance is more about sharing the risks. All the parties involved in this risk should figure out their responsibilities, and risk allocation; and share the risk accordingly

Risk Treatment and Risk acceptance are typical ways in the Cyber security domain. Cyber Security experts can enforce a kind of management to reduce the impact or probability of the threat. In some economical conditions it is not practical to do so. In this case the Cyberspace risk can be accepted. In the crisis of risk avoidance, one can decide not to execute the task that menaces them to the risk. Finally, Cyber security risk can be transferred to a third-party and in this situation Cyber insurance can be useful [8, 9].

6. RECENT CYBER ATTACKS

Past two years have been influenced by news of Cyber Attacks. Recently Cosmos bank has become a victim of one of the largest cyber attack. Attackers have duct off about 94 crores in just 2 days from various countries; it is done by malware attack on a bank server. Hackers have made clones of rupay and visa debit cards and transactions are made with the help of these clones. Wannacry, Petya, BSNL Malware attack, Mirai Botnet Malware, zomato are some of the examples of cyber crimes

“As per information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), beyond 53,000 cyber crimes took place in India in the year 2017; while about 22,207 Indian websites inclusive of 114 government websites were hacked during April 2017 to January 2018.”

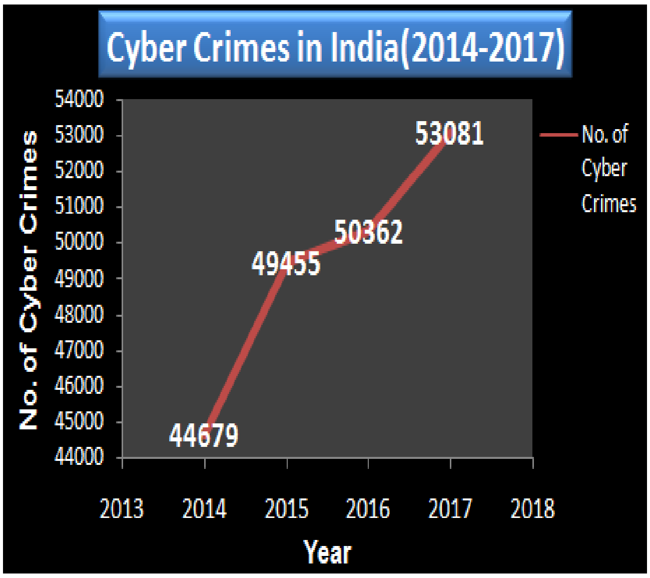

Fig 3: Cyber Crimes in India (2014-2017)

As the graph shows number of cyber crimes are rapidly goes on increasing [10].

7. CONCLUSION

Hackers are becoming more organized and cyber crimes are going on magnifying. So verify that your Cyber Security must be rigid, for this you must know about the possible risks of cyber attacks and the various faces of cyber attacks also. As we are suffering from these severe cyber attacks, just any security organization should not be responsible for the cyber security but everyone should aware of this.

8. REFERENCES

[1] V. A. Greiman, Professor, Boston University, USA “Cyber attacks: the fog of identity”, Electronic ISBN: 978-1-5090-5258-5,Print on Demand(PoD) ISBN: 978-1-5090-6172-3,INSPEC Accession Number: 16640583,Publisher: IEEE

[2] Rakesh Singh Kunwar,Priyanka Sharma,“Social media: A new vector for cyber attack”, Publisher: IEEE,Published in: 2016 International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Spring)

[3] Robert M. Clark, Simon Hakim editors,”Cyber Physical Security”,Protecting Critical Infrastructure at the State and Local Level,PP-22-25, ISBN 978-3-319-32822-5, ISBN 978-3-319-32824-9(eBook),© Springer International Publishing Switzerland 2017

[4] Dr.Shobha Bhardwaj, “Cyber securities and Cyber Terrorism”, Published on behalf of V.M. Open University, Kota,2015 ISBN-978-81-8496-580-3

[5] Jeff Melnick, “Top 10 Most Common Types of Cyber Attacks”, Published: May 15, 2018

[6] Jason Rivera, Forrest Hare, “The deployment of attribution agnostic cyber defense constructs and internally based cyberthreat countermeasures”, Publisher: IEEE, Published in: 2014 6th International Conference On Cyber Conflict (CyCon 2014),Tallinn, Estonia

[7] James Graham, Richard Howard, Ryan Olson, “CYBER SECURITY ESSENTIALS”, Auerbach Publications, ©Taylor and Francis Group

[8] G. Gonzalez-Granadillo, S. Dubus, A. Motzek, J. Garcia-Alfaro, E. Alvarez, M. Merialdo, S. Papillon, H. Debar,”Dynamic risk management response system to handle cyber threats”, ELSEVIER, Future Generation Computer Systems, Volume 83,2018,Pages 535-552,

[9] Krerk Piromsopa, Tomas Klima, Lukas Pavlik, “Designing Model for Calculating the Amount of Cyber Risk Insurance”, Publisher: IEEE, Published in: 2017 Fourth International Conference on Mathematics and Computers in Sciences and in Industry (MCSI),Corfu, Greece.

[10] “Over 53,000 cyber security incidents observed in 2017”,PTI,New Dehli. https://www.thehindubusinessline.com/info-tech/over-53000-cyber-security-incidents-observed-in-2017/article22705876.ece