*International Journal of Engineering Applied Sciences and Technology, 2020*
**Vol. 5, Issue 3, ISSN No. 2455-2143, Pages 280-282**
Published Online July 2020 in IJEAST (http://www.ijeast.com)

# HOW CYBER SECURITIES PLAY AN IMPORTANT ROLE FOR ANY ORGANIZATION

Santosh Kumar Sharma
BCA Student
Department Of Computer Science
Kalinga University, Atal Nagar, Chhattisgarh, India

Rahul Kumar Chawda
Assistant Professor
Department Of Computer Science
Kalinga University, Atal Nagar, Chhattisgarh, India

***Abstract- "Risk Can Never Be Removed, It Can Only Be Minimized."***

**Cyber Securities is most important part in our life, because today times your data sharing for mostly could networks and social media. There are millions of the users every day in social platform working, such as private companies, government companies, financial institutions and people's personal social accounts (Google Gmail, Facebook, Instagram, Twitter, What's app, LinkedIn etc.) Every day cyber-attack your account and personal data hacked then blackmails, account block and illegal modus change personal information. Other word cyber securities is secured our data and can be destroy for hackers mind.**

***Keywords-*** Cyber Security, Cyber-attack, Needs, Types, Scope.

## I. INTRODUCTION

"Cyber security is the production of digital assets are information system from attack are unauthorized access." The turn cyber security was coined "1998" as a result of one of the first were online resister virus "Morris Worm."

Cyber Securities means are secure you and your digital informations in cyberattack. Your securities issues for a organization's privacy, important data informations, companies informations, Government database, National important data's problems etc.

## II. SECURITY

Security means safety-guards. Today life security is very important because your every information's every data's link an online they are risky. Use as security camera, smart phones, smart key etc. But not 100 percent not secured, there are our life is totally dependent by Cyber Securities.

a. **Cyber Securities: -** A cyber security attempts to cyber-attacks it's pass the systems Securities, finding any weak points in the security that can be exploited by other cyber-attacker.

## III. THE COMMON CYBER-ATTACKS

A cyber-attack is a malicious and deliberate attempt by organizations to breach the information system of another organizations. The attacker seeks some type of benefit from disrupting the victim's network. Cybercrime has increased every year as people try to benefit from vulnerable business systems. Often, attackers are looking for ransom: 53 percent of cyber-attacks resulted in damages of $500,000 or more.

## IV. TYPES OF CYBER-ATTACKS

a. **Malware: -** Malware refers to the pieces of harmful coding which are uses to create different type of harmful software, such as virus and worms. There are Freezing(hang), Multiple File's, Duplicate File's, Encrypted Analysis, Automatically shortcuts etc.

b. **Phishing: -** Phishing means create fake pages designing or duplicate pages designing. It is a tactic we by attacker to reveal sensitive data just like credit card details, user id, password etc.

c. **Ransomware: -** Ransomware is a virus which encrypts the data on victims computer and demand for ransom to unlock the data. The motive for ransomware attacks is always for "Monetary gains".

d. **Spam: -** The unwanted mails or message's that companies send you to sell there products and services without permissions.

e. **Trojan horse: - "**Not self replicating but behaviors in virus mostly attack games.**"** Trojan horse is a small harmful software which, usually hide, inside gaming software. Trojan horse is a worm, but it acts like a virus.

f. **Spyware: -** Use to a spring in computers and others devices. There are spy's in monitor to system's. It is a harmful systems.

g. **Eaves – Dropping: - "**There are use to Monitoring**".** The act of monitoring communication between user without consent is called Eaves – Dropping.

h. **Hacking: -** A hacker is like a common man but his Thinking is out of common man thinking, they are expert in programming, networking, Operating Systems and applications, they may even their own hacking tools. The act of gaining illegal or ensuring unauthorized to any computers systems, network resources or online accounts by using venerability or bugs.

## V. SEVEN LAYERS OF CYBER SECURITIES

i. **Information Security Policies: -** There are the foundation of the security and well-being of our resources. They can help you increase the awareness of information security within your organizations.

ii. **Physical Security: -** We secure our valuables under lock and key and we monitor our homes with security cameras. It shouldn't be any different for our servers and offices. They provide to keep your system safe, with solutions that include everything from lockable racks to password-enabled screen savers.

iii. **Secure Networks and Systems: -** EGiS builds networks and systems with your company's security in mind. Our mission: to manage, monitor and protect the network that crucial intersection where your private network connects to the public Internet. We'll make sure you're DNS and domain name is safe, provide e-mail filtering, firewall and Internet content security and more.

iv. **Vulnerability Programs: -** Every system has inherent vulnerabilities. But by maintaining anti-virus, anti-spyware, anti-spam and Windows and firewall updates as well as updates to your industry programs.

v. **Strong Access Control Measures: -** There are safeguard against unauthorized access to your system by limiting and controlling access. We are using to complex passwords and multi-authentications.

vi. **Protect and Backup Data: -** It is very important part on layer. They are key to keeping your data safe is to encrypt it stored and when it's transported. Using continuous data protections make sure your backup data it changes.

vii. **Monitor and Test Your Systems: -** EGiS is here to test your internal and external systems for risks, review your policies with you and continually monitor and report.

## VI. UNDERSTAND THE NEED FOR SECURITY YOUR SYSTEM

"To catch an Attacker, think like an Attacker."

Its help to shore up an organization's defenses by attacking them himself, the results of the attack will them reveal what is safe and what need to be patched or reconfigured to improve security. Cyber Securities is basically an audit of the security systems of an organization.

## VII. SCOPE AND CHALLENGE FOR CYBER SECURITIES

- Cyber Securities is referred to as IT security's, the focused by computers, networks, programs and information from unauthorized access or duplicate issues.

- It's criminal activities computer network has led to the focus on sensitive information's or private data's, there are national security's issue.

- Scope for security's professionals in data protection.

- Today national security and business and personal data is totally depends on cyber security.

## VIII. WHY CYBER SECURITY IS NECESSARY

a) Cyber security is considering by an audit the organization's networking security.

b) Cyber security helped an organization's in identified weaknesses in the networking and helps by patch weaknesses.

c) Implementation by security patch in a networking minimize the Chance's of an attacks.

## IX. CONFIDENTIALITY, INTEGRITY AND AVAILABILITY TRIANGLE

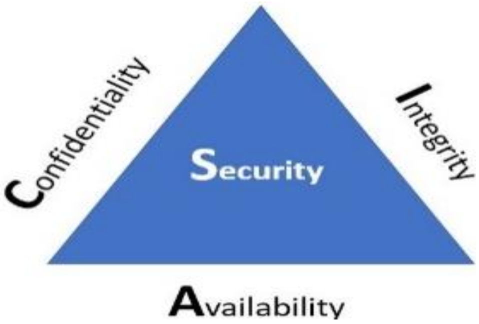

Fig 1.1 – Confidentiality, Integrity and Availability Triangle. (Image Credit: Google)

- Confidentially means security all information or data so that only authorized person can access it.
- Integrity means ensuring the informations should stay in its original from transmitted over the network.
- Availability means ensuring that the data stay available when even it is needed.

## X. CONCLUSION

The Cyber Securities is very important role of an Organizations, because variety of roles, context's, and used is very largest part of Nation.
Cyber Securities is a fields are very carefully and safety work by an organization, because it is more than weaknesses point's, issues, networks problems, devices hang issued, data's hacked etc. It is working by formal educations and businesses requirement's and government's works and personals and private information's.

## XI. ACKNOWLEDGEMENT

The Cyber Security's studied in India are in the early but very important phase. I was inspired, guided, mentored, supported and pushed by everyone around me. I hope to do justice by naming and thanking a few of them.

Mr. Nilesh Borkar Sir my Supervisor and Mr. Rahul Chawda Sir Assistant Professor has been the key person whose constant guidance and encouragement made this journey of research interesting. He stood by every single argument, discussion and conversation around the topic and skillfully pushed me to think broader and deeper. Without his complete support, this might have been an arduous task. I am indebted to him.

## XII. REFERENCES

1. K. Dinakar, R. Reichart, H. Lieberman, "Modeling the detection of textual cyberbullying", 2011.
2. M. Kaplan, M. Haenlein, "Users of the world unite! The challenges and opportunities of social media", Bus. Horizons, vol. 53, no. 1, pp. 59-68, 2010.
3. Kontostathis, L. Edwards, A. Leatherman, "Text mining and cybercrime" in Text Mining: Applications and Theory, Chi Chester, U.K.: Wiley, 2010.
4. A Cybersecurity Agenda for the 45th President. (2017, January 5).
5. Communications Security, Reliability and Interoperability Council. (2017). Final Report-Cybersecurity Workforce Development Best Practices Recommendations.
6. Hacking the Skills Shortage, A study of the international shortage in cybersecurity skills Center for Strategic and International Studies (2016). Santa Clara, CA: INTEL Security.
7. Japan data: William Roth, "Japan's Cybersecurity Market: Opportunities and Challenges," Sasakawa USA, February 12, 2016.
8. "National Cybersecurity Workforce Framework," National Initiative for Cybersecurity Education (NICE), November 2015.
9. Dance, Scott (20 May 2015). "Cyberattack affects 1.1 million CareFirst customers".
10. Atul M. Tonge, Suraj S. Kasture, Surbhi R. Chaudhari, "Cyber Crime and Security"International Journal of Advanced Research in Computer science and Software Engineering,2013, Vol 6,Issue 4,,Pages 46-52.