Cyber Attacks and Crimes in Cyber Security: A Comparative Analysis

Priti P. Tijare[1], Monika S. Shirbhate[2], Rupali Thakare[3]

[1,2,3]*Assistant Professor, CSE Dept, Dr. Rajendra Gode Institute of Technology & Research, Amravati, Maharashtra, India*

***

Abstract -*In the cutting edge world that is run through of utilizing technological knowledge and network connections, it is fundamental to know what cyber security is and to be prepared to effectively utilize it. Frameworks, significant documents, information, and other significant virtual things are in risk assuming that there is no security to watch it. Security is most secure method of assurance from various sorts of dangers and most organizations participate in the difficulties of safety particularly digital assaults. The attacks are expanding day by day, the examination study imply that likenesses and dissimilarities in the perceived digital protection regardless of whether it is an IT firm. Attackers improved hacking procedures and go for the weak point in the organizations out there. This paper center around the basic comparative analysis on cyber security, crimes, attacks and awareness & non awareness about cyber security among people in various organizations. It also discusses about safety of private computing against cyber crime and analyze about problems of cyber crimes which is faced by the people. Digital protection is critical on the grounds that military, government, monetary, clinical and organization associations and different gadgets. A crucial quota of the data can be sensitive information, whether that is financial data, property, personal information, or other various sorts of data for which illegal access or could ensure negative concerns.*

Key Words- Cyber Attack, Cyber Crime, Cyber Security, malware awareness, protection.

I. INTRODUCTION

The beyond couple of many years internet played significant role in worldwide communication and today it has almost about 3 billion users of internet, thus the internet has generated wide global network. We can't envision the existence without information technology exceeding half of the world population almost 58.8% used internet till 2019. Ratel Serbia reported 99.2% of people uses computer which is aged between 16 and 24 years and 98.2 % people uses internet every day [6]. At present government, non-government organization is going through cyber space and most essential information carry to this space and consequently it may lead to the cyber threats, cyber-attacks and cyber-crimes. The cyber posed the security to the government, we call it cyber security [9]. The cyber security originated in 1987. Cyber security is all about security protection through which we can protect the environment of user network, software application & also defending the computer network system which is connected to the internet and providing the protection to system from unnecessary attack [11]. Cyber-attacks includes trojan horse, spyware, sniffer, denial of services, virus, cream which is shown in figure 1. The cyber threats aims to gain illegal access damage data over the computer network like malware. Malware is malicious software huge amount of viruses and malware spreading all over a global like the internet worms, email viruses and keystroke, we can enlarge our computer performance by detaching the spyware [8]. Ransomware software encodes our computer data and request to payment to decode for reinstate files, 80% of our computers are infected by such kind of spyware [1]. Analyzing the need of security for the software application because there are threats in cyber- attacks they puts high risk in software for losses the data or information so it can be difficult to recover the data or information [7].

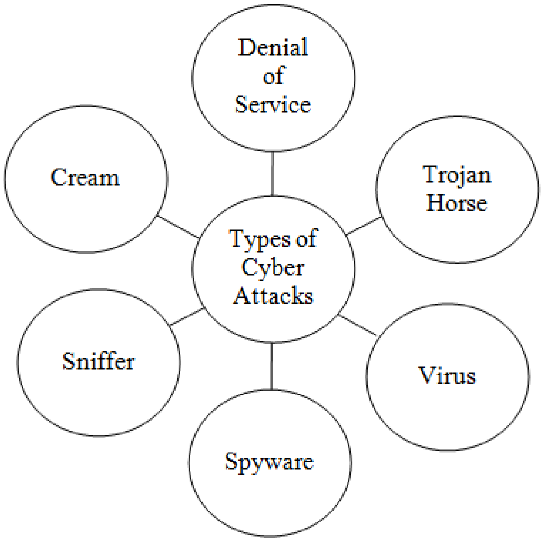

Fig 1: Types of attacks

Although some user does not aware about the security risk they don't have any idea how to accomplish the cyber security even if they are aware about phishing attack, malware attack [6]. Cyber security is shared authority internet and also everyone who make use of internet for any other reason which is private or the personal reason and the Internet corporation can also a make a contribute by using protection of their community and payment processes. The government should be aware and also instruct to enforce anti crime law [8].

II. LITERATURE REVIEW

There have been several papers which are highlighting the use of cyber security, the attributes of threats and also the vulnerability in cyber safety are exceptional from information security. All safety is worried with variety of threats for resources [2]. The author [6] has suggested the data which is having some quite proper facts about the cyber protection, whichever participant has no longer to be confident about cyber safety in the various institution and awareness and non awareness about protection of their non-public data from unauthorized users.

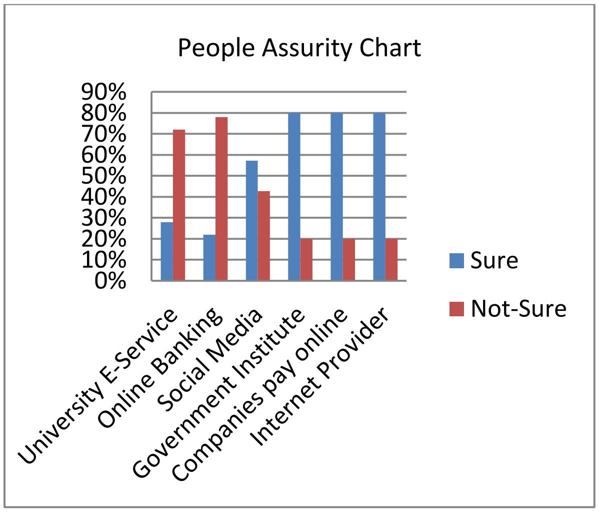

Fig 2: People assurity

For safety, the private computing can be carried out following anti cyber-crime policies.

- Scan the executable archive downloaded at once as from the net before using it.
- Document and spreadsheet can also include the spyware so avoid it.
- Virus also scan the electronic mails as well as attachments earlier than opening it.
- Even if your personal computer is attacked by using any virus, malware, disconnect your pc immediately from network and do away with it with the help of IT security department.
- RTF files [Rich Text Format] is about secure structure to keep away from virus because the doc file can be hacked by easily without any problem by micro viruses [1].

According to the researcher, from 2018 to 2021 cyber-crime has expanded on the global degree the researcher has point out average of cyber-crime cases in the world.

The below figure 3 shows that cyber-crime is not only a national but international fact. The reliable growth has aims to multi responsible society along with the cyber safety infrastructure [5]. According to the author [10] there are three most important feature of cyber security.

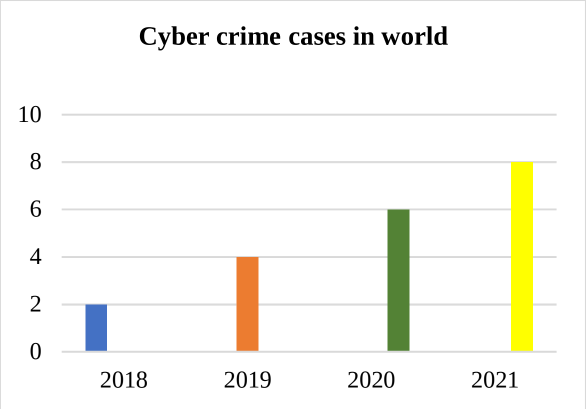

Fig 3: Average cyber-crime in the world

People: Every worker should aware about their role to prevent cyber threat.

Technology: From access manipulate to installing the antivirus, technology utilize to decrease cyber risk.

Process: Documented approaches need to be clearly determining role, responsibility and procedures. The relevant researcher discussed about their rules and precautions for internet banking because there are high risk of cyber-crime in online transaction. User must be changed their password in every three months. Use public gadgets for internet banking as incredibly irresponsible. Bank should be force to their customers for changing the password and verify that there is no repetition as a final two passwords [8]. According to author [2], the cyber-crimes are classified into three types like emails that trouble someone and spyware software to crack anybody's computer unlawfully and unauthorized access gain the personal data and also the plagiarizing exclusive records.

III. PROBLEM ANALYSIS

In today's world the cyber security is widely used in the worldwide because of the cyber-attack and cyber- crime increases day by day. The average people of the information technology not always have a technically educated and most likely no longer to be studied cyber security in his/her past education. People choose much less secure password because problematic password has too hard to remember, this shows important reality of majority of users are not aware about how to choose accurate and unique password that cannot be easily hacked by someone. In today's generation all people have smart phones but only few people install antivirus into their phone. Others are used public wi-fi that becomes more problematic. The attacker can attack easily. Following are the problems to achieve cyber security as mentioned below.

- Non updates of software application to secure the system.
- Not installing the antivirus to prevent from malicious software.
- Use of less secure and easy password that unknown person may crack password easily.
- Use of public wifi or network.

Around 12.2% people are using the public wifi for online purchase and 6.1% for online banking and the 60.5% used for sending mails so it can easily attack by hackers and people do not even know about this [6]. This all problems may affect the cyber security. This all problems needs to be fixed and it is important for our security purpose so we can aware and secure from the cyber-attack as well as cyber-crime so the unknown person cannot get unauthorized access and cannot hack our legal information, we may safe form all the unknown attacks.

IV. COMPARATIVE ANALYSIS

In this section, we analyze different methods, challenges, strength and weakness that other authors used for achieving the cyber security as follow.

I] Paper title /author: Cyber Security at Software Development Time / Mark Bradley, Ansgar Fehnker, Ralf Huuck[3].

Methods: Gonna static analysis tool, tree-based pattern matching to model checking.

Challenges: Real security issue detection.

Strength: Highlighted importance of secure source code for developing for the secure system and improving cyber security.

Weakness: Only on focuses the implementation phase of software does not create the simple task for SDLC.

II] Paper title/ author: Analyzing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach / Abdul wahid khan, shah zaib, faheem khan, ilhan, tarimer jung taek seo, and jiho shin [2]. **Method**: Cyber-security challenge model (CSCM), Snow bowling technique, and the pattern-baseddetection algorithm.

Challenges: Critical cyber security challenge for companies.

Strength: Identification of security threats in the various organization like as the Pattern based detection algorithm with assure continuous security observing. **Weakness**: Cost security issue that serious economic investment & financial issue in organization.

III] Paper title/ author: Cyber Security: The State of the Practice in Public Sector Companies in India / T. R. Srinivas, G. Vivek [4].

Method: By conducting the survey through the participant and did contribution to that work including the workshop in may 2014 management. developmentprogram (MDP).

Challenges: Security issue, awareness about cyber security.

Strength: Motivated to the people improving the level of cyber security through the conducting survey.

Weakness: Does not conducting the training of the awareness of cyber risks and responding ratings of peoples who doesn't aware about firewall protection 57% scan of malware 3.6% and the 10.7% is awareness of cyber risk.

IV] Paper title/ author: A Bird's Eye View of Cyber Crimes and Free and Open Source Software's to Detoxify Cyber Crime Attacks – an End User Perspective / M. K. Jayanthi Kannan [1].

Method: Providing the steps for the installation of spyware in system. Methods for deleting the spyware viruses & worms. Ex: software for antivirus security, email alert service box.

Challenges: Accessing the cyber security.

Strength: Protecting the personal laptop, desktop computer by installing antivirus security software will prevents from spreading of malware by providingvarious steps.

Weakness: There is a no method or steps for updatingthe antivirus or the software application. If the users already have a antivirus they does not aware about updating the antivirus.

V] Paper title/ author: Systematic Mapping Study on Security Approaches in Secure Software Engineering

/ Rafiq Ahmad Khan, Siffat Ullah Khan, Habib UllahKhan, Muhammad Ilyas [7].

Method: Stages- SMS process, SSE method.

Challenges: Systematic software security.

Strength: Maintaining the security features like privacy, integrity, understanding secure software methods that can be leads with attacks, providing the concept about there are only 10.70% of peoples are aware about the cyber risk and 2% of training of awareness about cyber risk, 32.10% are responded that having appropriate software security.

Weakness: It also needs to be combined with the powerful tools for implementation plan.

According to the survey [4] anti-malware policy and practices. The following figure 4 and figure 5 shows the responding ratings of awareness of cyber risk and related training and responding ratings of malware protection and aware about scanning of malware. So the overall awareness levels and the necessary training are comparatively poor. In case of scanning for malware in network situation is pathetic as only 3.6% of the participants are aware. This is all about the comparative analyze regarding the cyber security.

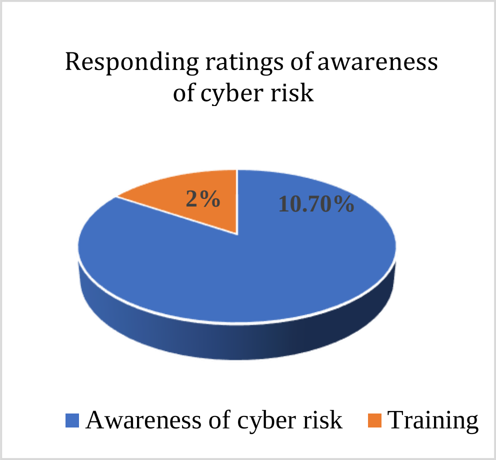

Fig 4: Ratings of awareness

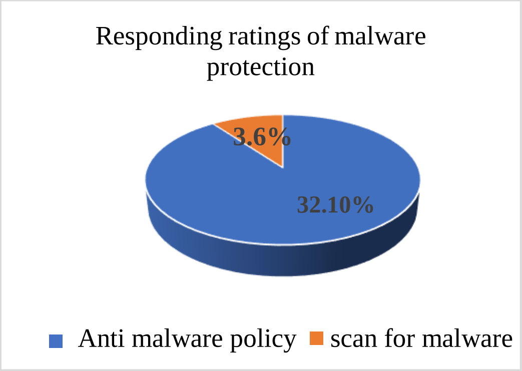

Fig 5: Ratings of malware protection

V. CONCLUSION

Everyone wants to be secure and safe while using internet but times have come to make this sure of cyber-attacks and cyber crimes. Based on this analysis of cyber security we identified the different kind of cyber-attacks. We have gone through the comparative analysis on cyber security that includes the methods, challenges, strength, weakness & also identify theresponding ratings of awareness of cyber risk & malware protection. Day by day the cyber-crimes are increasing that may lead to the biggest challenge of securing the information for the organization. Therefore an increased awareness of cyber-attacks among individuals and organizations is vital so that solutions can be found quickly. We also get surety about how many people are aware and non aware about the cyber security in various organizations. Future exploration focus needs to be on the development of a secure and secure internet terrain of the coming generation.

REFERENCES

[1]. M. K. Jayanthi Kannan, "A Bird's Eye View of Cyber Crimes and Free and Open Source Software's to Detoxify Cyber Crime Attacks – an End User Perspective", 2017 2nd International Conference on Anti Cyber Crimes (ICACC), ©2017 IEEE.

[2]. Khan, Abdul Wahid, Zaib, Shah, Khan, Faheem, Tarimer, Ilhan, Seo, Jung Taek, Shin, Jiho, "Analyzing and Evaluating Critical Cyber Security Challenges Faced by Vendor Organizations in Software Development: SLR Based Approach", IEEE Access, vol. 10, pp. 65044- 65054, 2022.

[3]. M. Bradley, A. Fehnker and R. Huuck, "Cyber security at software development time, Defence Science Research Conference and Expo (DSR), pp. 1- 4, September 2011.

[4]. T. R. Srinivas and G. Vivek, "Cyber security: The state of the practice in public sector companies in India," International Conference on Computing and Communication Technologies, 2014, pp. 1-5, March 2015

[5]. Arti, Rani, Reena, "Cyber Security in Digital Society: Indian Perspective", UGC CARE Group 1, ISSN: 2277-7067, vol. VII, Issue 2(III), pp. 44-48, 2021-2022.

[6]. Kovacevic, Ana, Putnik, Nenad, Toskovic, Oliver, "Factors Related to Cyber Security Behavior", IEEE Access, no. 21693536, vol. 8, pp. 125140-125148, July 8, 2020.

[7]. Khan, Rafiq Ahmad, Khan, Siffat Ullah, Khan, Habib Ullah, Ilyas, Muhammad, "Systematic Mapping Study on Security Approaches in Secure Software Engineering", IEEE Access, no. 21693536, vol. 9, pp. 19139- 19160, January 18, 2021.

[8]. Mallika, Vikas Deep, Purushottam Sharma, "Analysis and Impact of Cyber Security Threats in India using Mazarbot Case Study", Proceedings of the International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS-2018): 21 -23 December 2018, Belagavi, India, pp. 499-503, ©2018 IEEE.

[9]. Li, Yuchong, Liu, Qinghui, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments", Energy Reports, no. 23524847, vol. 7, pp. 8176- 8186, © 2021.

[10]. Das, Ayan, Dawn Saju, Dr. Neha Gupta, "A Study of Cyber Security and Its Challenges", International Journal of Engineering Applied Sciences and Technology, no. 2455-2143, vol. 5, Issue 1, pp.747-753, May 2020.

[11]. Adiba Shaikh, Arshiya A. Khan, Syed Zebanaaz, Shazia Shaikh, Nazneen Akhter, "Exploring Recent Challenges In Cyber Security And Their Solutions", International Journal of Creative Research Thoughts (IJCRT), ISSN: 2320- 2882, vol. 9, no. 12, pp. 603-604, 2 December 2021.